明 細 書

通信装置、通信システム及び認証方法

技術分野

[0001] 本発明は、通信装置、通信システム及び認証方法に関し、より特定的には、無線LAN等による通信装置間の認証接続におけるセキュリティの向上と設定の簡単化とを両立させた通信装置、及びその通信装置を構成に含む通信システム、並びにその通信システムで行われる認証方法に関する。

背景技術

[0002] 近年、無線LAN技術の進展に伴い、家庭内等で無線LANの普及が進んできている。しかし、無線LANは、有線LANに比べて面倒な配線接続が必要ない代わりに、無線接続のための種々の設定が必要となる。特に、無線LANの必須項目であるセキュリティに関する設定は、内容が専門的かつ複雑であるため、技術に詳しくない一般ユーザにとっては、困難な設定作業になってしまっているのが現状である。例えば、IEEEスタンダード802．11iでは、認証と鍵生成という2つの部分からなる接続処理が規定されており、クライアントと認証サーバ又はアクセスポイント(AP)が予め認証用の共通情報を持っていることが前提となる。このため、家庭内で無線LANをさらに普及させるためには、設定を簡単化させるという課題は避けて通れない課題の1つとなっている。

この課題を解決させるために考案された従来の方法を、以下に簡単に説明する。

[0003] 第1の方法は、無線通信を用いてAPとクライアントとの間で相互認証を行うための方法である(特許文献1を参照)。この第1の方法では、両方に設置されているボタンを同時に押して双方の無線出力パワーを下げ、特別な設定モードに入って自動的に設定を行う。この第1の方法は、無線出力パワーをコントロールすることで、APとクライアントとの間に一種の秘密通信を形成し、相互認証及び設定を行うものである。

[0004] 第2の方法は、無線通信を用いてマスタとスレーブとの間で相互認証を行うための方法である(図35、特許文献2を参照)。この第2の方法では、マスタとスレーブとで事前に共通鍵を共有させる。認証開始時には、スレーブからマスタへ認証要求が送

信される。マスタは、チャレンジ指示をスレーブに送信する。スレーブは、共通鍵で暗号化されたチャレンジを含む認証要求をマスタに送信する。マスタは、暗号化されたチャレンジを自己の共有鍵で復号し、復号したものがスレーブに送信済みのチャレンジと一致する場合、ユーザの指示に従って認証許可／認証不許可の応答をスレーブに返信する。

[0005] 第3の方法は、無線通信を用いてマスタとスレーブとの間で相互認証を行うための方法である(図36、特許文献3を参照)。この第3の方法では、マスタとスレーブとで登録ボタンの押し下げを受け付ける。スレーブは、自己の公開鍵と固有情報とを含む登録申請を、マスタに送信する。マスタは、スレーブの公開鍵で暗号化されたスレーブの固有情報を含む登録確認を、スレーブに送信する。続いて、マスタは、スレーブの公開鍵で暗号化されたマスタの共通鍵を含む認証通知を、スレーブに送信する。スレーブは、マスタの共通鍵で暗号化された認証応答を含む認証受領を、マスタに送信する。

[0006] 第4の方法は、無線通信を用いて表示手段を有する2つの通信装置間で相互認証を行うための方法である(図37、特許文献4を参照)。この第4の方法では、通信装置Aは、自己の公開鍵を含む鍵伝送メッセージを、通信装置Bに送信する。この公開鍵は、通信装置A及び通信装置Bにおいてそれぞれ他の値に変換されて、各々の視覚手段又は聴覚手段を用いて出力される。ユーザは、出力された公開鍵の変換値が一致するか否かを検証し、許可／不許可を判断する。許可されれば、通信装置Bは、通信装置Aの公開鍵で暗号化された新しい鍵生成情報を、通信装置Aに送信する。そして、通信装置A及び通信装置Bは、新しい鍵生成情報に基づいて通信用の共通暗号鍵を生成する。

特許文献1:特開2004－215232号公報

特許文献2:特許第3585422号明細書

特許文献3:特許第3628250号明細書

特許文献4:特許第3552648号明細書

発明の開示

発明が解決しようとする課題

[0007] しかしながら、上記第1の方法では、無線電波が届く範囲に同種の無線LANインタフェイスを装着している他のクライアントが存在する場合、この他のクライアントと接続してしまう危険を完全に排除することができない。偶然に、隣家で同じ設定を行っている可能性があるからである。また、第1の方法では、表示手段を通してユーザによる確認をしないまま相互認証が自動で行われてしまうという問題がある。

[0008] また、上記第2の方法では、共有する共通鍵を入力するために、キーボード等の入力手段が必要になる。このため、キーボード等を持たないネット家電(Networked Consumer Electronics)には不向きである。

[0009] また、上記第3の方法では、登録申請処理において不正な第三者(Man-in-the-Middle)が存在する場合、この第三者による公開鍵の改竄による「なりすまし行為」を防止することができない。

[0010] さらに、上記第4の方法では、通信装置A及び通信装置Bの両方に表示手段を備える必要がある。また、公開鍵の変換値の表示と検証をするだけでは、ユーザの目又は耳では区別しにくい似た様な変換値を持つ他の公開鍵に改竄されることによって、不正な第三者によるなりすまし行為が生じる可能性が残る。

[0011] それ故に、本発明の目的は、不正な第三者によるなりすまし行為を防止し、認証処理の安全性及び確実性を向上させた通信装置、通信システム及び認証方法を提供することである。

課題を解決するための手段

[0012] 本発明は、他の通信装置から接続のための認証を要求される通信装置、他の通信装置へ接続のための認証を要求する通信装置、これらの通信装置で構成されるシステム、及びこのシステムで実行される認証方法に向けられている。

[0013] 上記目的を達成させるために、本発明の認証を要求される通信装置は、通信装置を一意に特定できる装置情報を含む認証要求を他の通信装置から受信する受信部と、認証要求に含まれる装置情報を画面に表示する表示部と、表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、入力部に入力された指示に従って、他の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備える。

[0014] また、本発明の認証を要求する通信装置は、通信装置を一意に特定できる装置情報を含む認証要求を他の通信装置へ送信する送信部と、認証要求に対応した装置情報を含む認証応答を他の通信装置から受信する受信部と、認証応答に含まれる装置情報を画面に表示する表示部と、表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、入力部に入力された指示に従って、他の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備える。

[0015] 本発明は、上記認証を要求される通信装置又は認証を要求する通信装置のいずれか一方に、表示装置を備えればよい。

[0016] 受信部が、複数の他の通信装置から複数の認証要求又は認証応答を受信した場合、表示部は、当該複数の認証要求又は認証応答に含まれる複数の装置情報を画面に同時に表示すればよい。また、認証部は、所定時間の経過時に入力部へユーザ指示がなければ、他の通信装置を認証不許可にする処理を実行してもよい。なお、典型的な装置情報には、通信装置の識別番号、及び公開鍵又は電子署名の何れかが、少なくとも含まれる。好ましくは、認証部において、他の通信装置から受信した認証要求に含まれる識別番号を用いて、共通暗号鍵を生成される。

発明の効果

[0017] 上記の本発明によれば、認証要求してきたスレーブの装置情報をマスタ側で、又はマスタ側の装置情報をスレーブ側で画面表示させる。これにより、ユーザが、認証要求を送信してきた通信装置が認証許可すべきスレーブ又はマスタであるか否かを、容易に判断することが可能となる。従って、認証処理の安全性及び確実性を向上させることができる。また、画面で確認された装置情報(ID)を用いて共通暗号鍵を生成すれば、実通信における秘匿性をさらに向上させることができる。

図面の簡単な説明

[0018] [図1]図1は、本発明の第1の実施形態に係る無線LANシステムの概要構成を示す図である。

[図2]図2は、二者間で行われる基本的な認証手順を示すシーケンス図である。

[図3]図3は、本発明の第1の実施形態に係る認証方法の処理を示すフローチャートである。

[図4A]図4Aは、認証要求の一例を示す図である。

[図4B]図4Bは、認証応答の一例を示す図である。

[図5A]図5Aは、表示部13の画面表示例を示す図である。

[図5B]図5Bは、表示部13の画面表示例を示す図である。

[図6]図6は、三者間で行われる認証手順を示すシーケンス図である。

[図7]図7は、表示部13の画面表示例を示す図である。

[図8]図8は、二者の間に不正者が割り込む場合の認証手順を示すシーケンス図である。

[図9]図9は、本発明の第2の実施形態に係る無線LANシステムの概要構成を示す図である。

[図10]図10は、二者間で行われる基本的な認証手順を示すシーケンス図である。

[図11]図11は、本発明の第2の実施形態に係る認証方法の処理を示すフローチャートである。

[図12A]図12Aは、認証要求の一例を示す図である。

[図12B]図12Bは、認証応答の一例を示す図である。

[図12C]図12Cは、鍵生成要求の一例を示す図である。

[図12D]図12Dは、鍵生成応答の一例を示す図である。

[図13]図13は、三者間で行われる認証手順を示すシーケンス図である。

[図14]図14は、二者の間に不正者が割り込む場合の認証手順を示すシーケンス図である。

[図15]図15は、認証部12及び22の詳細な構成例を示す図である。

[図16]図16は、本発明の第3の実施形態に係る認証方法の処理を示すフローチャートである。

[図17]図17は、認証要求メッセージのフォーマットの一例を示す図である。

[図18]図18は、認証応答メッセージのフォーマットの一例を示す図である。

[図19]図19は、改竄・転送された認証要求メッセージのフォーマットの一例を示す図である。

[図20]図20は、改竄・転送された認証応答メッセージのフォーマットの一例を示す図

である。

[図21]図21は、認証応答メッセージのフォーマットの一例を示す図である。

[図22]図22は、改竄・転送された認証応答メッセージのフォーマットの一例を示す図である。

[図23]図23は、共通暗号鍵生成要求メッセージのフォーマットの一例を示す図である。

[図24]図24は、共通暗号鍵生成応答メッセージのフォーマットの一例を示す図である。

[図25]図25は、他の実施形態に係る無線LANシステムで行われる認証手順を示すシーケンス図である。

[図26]図26は、他の実施形態に係る無線LANシステムで行われる認証手順を示すシーケンス図である。

[図27]図27は、AP間のクライアントのID情報共有の動作手順を示すシーケンス図である。

[図28]図28は、クライアントのID情報共有の場合のAPとクライアントとの認証動作を示すシーケンス図である。

[図29]図29は、AP間のクライアントのID情報共有の場合の認証動作のシーケンス図である。

[図30]図30は、クライアントのID情報をルータで共有する実施形態を示すシーケンス図である。

[図31]図31は、クライアントのID情報をルータで共有する実施形態の場合の認証動作を示すシーケンス図である。

[図32]図32は、接続切断によりクライアントの認証済みID情報を消去する動作を示すシーケンス図である。

[図33]図33は、接続切断により複数のAP上のクライアント認証済みID情報を消去する動作を示すシーケンス図である。

[図34]図34は、接続切断によりルータ上のクライアント認証済みID情報を消去する動作を示すシーケンス図である。

[図35]図35は、従来の認証方法の処理例を示すフローチャートである。

[図36]図36は、従来の認証方法の処理例を示すフローチャートである。

[図37]図37は、従来の認証方法の処理例を示すフローチャートである。

符号の説明

[0019] 10、40 マスタ(AP)

11、21 送受信部

12、22 認証部

13、23 表示部

14、24 入力部

20、50 スレーブ(クライアント)

30 無線LAN

90 不正者装置

111 公開鍵・秘密鍵生成部

112 電子署名部

113 暗号化部

114 復号部

115 擬似乱数発生部

116 ハッシュ関数部

117 共通暗号鍵生成部

発明を実施するための最良の形態

[0020] 本発明は、無線／有線及び近距離／遠距離を問わず、様々なネットワークシステムに接続される通信装置を提供するものであり、特にその通信装置間で行われる認証処理に特徴がある。以下、マスタ(又はアクセスポイント)とスレーブ(又はクライアント)とを含む無線LANシステムを一例に挙げて、本発明を説明する。

[0021] (第1の実施形態)

図1は、本発明の第1の実施形態に係る無線LANシステムの概要構成を示す図である。図1の無線LANシステムは、マスタ10とスレーブ20とが、無線LAN30で接続される構成である。マスタ10は、送受信部11と、認証部12と、表示部13と、入力部1

4とを備える。スレーブ20は、送受信部21と、認証部22と、入力部24とを備える。

[0022] 送受信部11は、認証部12から認証メッセージを受け、スレーブ20のアドレスとマスタ10のアドレス等のスレーブ20が受信するために必要な情報をヘッダとして付け加えた後、無線LAN30により送信する。また、送受信部11は、スレーブ20から送信されたメッセージをヘッダ情報によりマスタ10宛であるかを判断して受信し、認証メッセージ部分を取り出して認証部12に渡す。送信と受信に使用された無線LAN30の通信における無線チャンネル情報(例えば、チャンネル番号)は、それぞれ認証部12に通知される。同様に、送受信部21は、認証部22から認証メッセージを受け、マスタ10のアドレスとスレーブ20のアドレス等のマスタ10が受信するために必要な情報をヘッダとして付け加えた後、無線LAN30により送信する。また、送受信部21は、マスタ10から送信されたメッセージをヘッダ情報によりスレーブ20宛であるかを判断して受信し、認証メッセージ部分を取り出して認証部22に渡す。送信と受信に使用された無線チャンネル情報は、それぞれ認証部22に通知される。

[0023] 認証部12及び22は、他の通信装置との接続時に全体的なコントロールをする役割を果たす。また、認証部12及び22は、認証要求等のメッセージの組み立てと分解処理とを行う。認証部12及び22は、認証要求メッセージの第三者装置による改竄・転送への監視を行う。認証部12は、さらにチャンネル情報表示又は公開鍵表示等のコントロールも行う。この認証部12及び22は、無線LANのMAC(メディア・アクセス・コントロール)レイヤ又はMACよりも上位のレイヤのどちらに実装されてもよい。MACレイヤに実装される場合、認証要求メッセージ等はMACレイヤのフレームと同じような形式を使用する。一方、MACよりも上位のレイヤに実装される場合、認証要求メッセージ等はMACレイヤのフレームと異なった形式を使用し、MACフレームにカプセルされた形で送信される。

[0024] 表示部13は、スレーブ20から受信した認証要求に含まれている装置情報を画面に表示する。装置情報とは、例えば、製品番号やMACアドレス等からなる識別番号(ID)、公開鍵、電子署名等である。この表示は、ユーザに認証許可/認証不許可の判断をさせるために行われる。表示部13は、液晶等の表示デバイスである。

[0025] 入力部14は、ユーザによるマスタ10に対するデータ入力やコマンド入力に加え、

表示部13の表示に基づく認証許可／認証不許可の判断を入力するために設けられる。入力部24は、ユーザによるマスタ10に対するデータ入力及びコマンド入力するために設けられる。この入力部14及び24は、例えば押しボタンで構成される。

[0026] この第1の実施形態は、マスタ10だけが表示部13を備えている無線LANシステムに関する実施形態である。例えば、スレーブ20が表示部のないネットワークカメラであり、マスタ10が表示部13のあるネットワークカメラコントローラである場合が考えられる。以下、この第1の実施形態に係る無線LANシステムで行われる認証手順を説明する。なお、認証部12及び22がMACレイヤに実装される場合、マスタ10とスレーブ20との間でやり取りされる電文の形式には、IEEEスタンダード802．11のMACレイヤ規格等の既知の形式が利用できる。

[0027] 以下、図2～図8を用いて、第1の実施形態におけるマスタ10とスレーブ20との間で行われる認証手順を、様々なケースに分けて説明する。

[0028] (1)二者間で行われる基本的な認証手順(図2)

マスタ10との認証を行う場合、スレーブ20は、装置情報としてID及び公開鍵(又は電子署名)を含む認証要求を、マスタ10に送信する(ステップS311)。図4Aは、認証要求の一例を示す図である。マスタ10は、認証要求を受信し(ステップS301)、その認証要求に含まれる装置情報を表示部13の画面に表示させる(ステップS302)。図5A及び図5Bは、装置情報が表示された表示部13の画面例を示す図である。ユーザは、表示部13の画面に表示されている装置情報を目視確認し、入力部14を介して認証許可又は認証不許可を判断してマスタ10に指示する(ステップS303)。この指示は、典型的には押しボタンを押し下げることによって行われる。認証許可／認証不許可を指示されたマスタ10は、指示に従った応答をスレーブ20へ送信する(ステップS304、S305)。

[0029] なお、認証許可／認証不許可を判断するためには、ユーザが、スレーブ20の装置情報を入手しておく必要がある。スレーブ20の装置情報は、マスタ10の表示部13を確認するユーザ自らが直接入手(スレーブ20の内部メモリデータや製品仕様書等から入手)してもよいし、スレーブ20を管理する他のユーザから通知(電話やメモ書き等による通知)してもらうようにしてもよい。また、入手のタイミングは、マスタ10の表示部

13に情報が表示された時であってもよいし、その表示よりも前であってもよい。

[0030] 表示部13の画面に表示されている装置情報が正しいとユーザに判断されて認証許可が指示された場合、マスタ10は、スレーブ20の公開鍵で暗号化された自己のIDと乱数とを含む認証許可応答を作成し、スレーブ20へ送信する(ステップS304)。図4Bは、認証応答の一例を示す図である。この認証許可応答は、スレーブ20で受信される(ステップS312)。その後、マスタ10及びスレーブ20は、スレーブ20の公開鍵(PubKey)、マスタ10のID(IDm)、スレーブ20のID(IDs)、及び乱数(N)に基づいて、通信用の共通暗号鍵をそれぞれ生成する(ステップS306、S313)。通信用の共通暗号鍵は、例えば以下の式で生成される。但し、prf()は、擬似乱数関数である。また、PreMasterKeyは、予め設定された共通値である。

共通暗号鍵 = prf(PreMasterKey, PubKey||IDm||IDs||N)

[0031] 一方、表示部13の画面に表示されている装置情報が誤っているとユーザに判断されて認証不許可が指示された場合、マスタ10は、認証不許可応答を作成してスレーブ20へ送信する(ステップS305)。なお、スレーブ20が、認証要求を送信した後所定時間内にマスタ10から応答がなければ、認証不許可と判断するようにしておけば、マスタ10は、認証不許可応答をスレーブ20へ送信しなくてもよい。

[0032] (2)三者間で行われる認証手順(図6)

これは、第1のスレーブ20が、装置情報[ID1、鍵1]を含む認証要求をマスタ10に送信すると同時に、第2のスレーブ20が、装置情報[ID2、鍵2]を含む認証要求をマスタ10に送信するケースである。この場合、マスタ10は、2つの認証要求を受信して2つの装置情報を表示部13の画面に表示させる。図7は、装置情報が表示された表示部13の画面例を示す図である。ユーザは、表示部13の画面に表示されている2つの装置情報を目視確認し、入力部14を介して認証許可又は認証不許可を判断してマスタ10に指示する。もちろん、ユーザは、認証許可すべきスレーブ20の装置情報を知っているので、その装置情報を送信してきたスレーブ20を選択して、認証許可を行う。なお、表示部13の画面に表示された何れの装置情報も既知の装置情報と一致しなければ、ユーザは、認証不許可を判断する。

なお、上述した認証処理は、四者間以上で行われる場合も同様である。また、鍵に

代えて電子署名を装置情報に用いても同様に行われる。

[0033] (3)二者の間に不正者が割り込む場合の認証手順(図8)

スレーブ20は、装置情報[ID1、鍵1]を含む認証要求をマスタ10に送信する。しかし、この認証要求は、マスタ10へ届かずに不正者装置90に受信される。不正者装置90は、スレーブになりすますために、装置情報[ID1、鍵1]を偽装置情報[ID1、鍵2]に付け替えた認証要求を、マスタ10に送信する。マスタ10は、認証要求を受信し、その認証要求に含まれる装置情報を表示部13の画面に表示させる。ユーザは、表示部13の画面に表示されている装置情報を目視確認し、表示されている装置情報のうち、公開鍵情報が認証許可すべきスレーブ20の装置情報と一致しないことを判断する。すなわち、ユーザは、表示された装置情報[ID1、鍵2]が、入手していたスレーブ20の装置情報である[ID1、鍵1]と異なることを認識する。これに応じて、ユーザは、認証要求してきた装置に対して認証不許可の応答を送信する。なお、鍵に代えて電子署名を装置情報に用いても同様に行われる。

[0034] 以上のように、本発明の第1の実施形態に係る通信装置によれば、認証要求してきたスレーブの装置情報をマスタ側で画面表示させる。これにより、ユーザが、認証要求を送信してきた通信装置が認証許可すべきスレーブであるか否かを、容易に判断することが可能となる。従って、認証処理の安全性及び確実性を向上させることができる。

また、画面で確認された装置情報(ID)を用いて共通暗号鍵を生成すれば、実通信における秘匿性をさらに向上させることができる。

[0035] (第2の実施形態)

図9は、本発明の第2の実施形態に係る無線LANシステムの概要構成を示す図である。図9の無線LANシステムは、マスタ40とスレーブ50とが、無線LAN30で接続される構成である。マスタ40は、送受信部11と、認証部12と、入力部14とを備える。スレーブ50は、送受信部21と、認証部22と、表示部23と、入力部24とを備える。図9でわかるように、第2の実施形態に係る無線LANシステムは、マスタ40側ではなくスレーブ50側に表示部23を備えた構成である。

以下、この異なる構成部分を中心に第2の実施形態を説明する。

[0036] 表示部23は、マスタ40から受信した認証応答に含まれている装置情報を画面に表示する。この表示は、ユーザに認証許可／認証不許可の判断をさせるために行われる。表示部23は、液晶等の表示デバイスである。入力部24は、ユーザによるスレーブ50に対するデータ入力やコマンド入力に加え、表示部23の表示に基づく認証許可／認証不許可の判断を入力するために設けられる。

[0037] この第2の実施形態は、スレーブ50だけが表示部23を備えている無線LANシステムに関する実施形態である。例えば、スレーブ50が表示部23のあるWiFi電話子機であり、マスタ40が表示部のないWiFi電話親機である場合が考えられる。以下、この第2の実施形態に係る無線LANシステムで行われる認証手順を説明する。なお、認証部12及び22がMACレイヤに実装される場合、マスタ40とスレーブ50との間でやり取りされる電文の形式には、IEEEスタンダード802．11のMACレイヤ規格等の既知の形式が利用できる。

[0038] 以下、図10～図14を用いて、第2の実施形態におけるマスタ40とスレーブ50との間で行われる認証手順を、様々なケースに分けて説明する。

[0039] (1)二者間で行われる基本的な認証手順(図10)

マスタ40との認証を行う場合、スレーブ50は、認証要求をマスタ40に送信する(ステップS1111)。図12Aは、認証要求の一例を示す図である。マスタ40は、認証要求を受信し(ステップS1101)、自己のID及び公開鍵(又は電子署名)の装置情報を含む認証応答を、スレーブ50に送信する(ステップS1102)。図12Bは、認証応答の一例を示す図である。スレーブ50は、認証応答を受信し(ステップS1112)、その認証要求に含まれる装置情報を表示部23の画面に表示させる(ステップS1113)。表示部23の画面表示例は、図5A及び図5Bに示した通りである。ユーザは、表示部23の画面に表示されている装置情報を目視確認し、入力部24を介して認証許可又は認証不許可を判断してスレーブ50に指示する(ステップS1114)。この指示は、典型的には押しボタンを押し下げることで行われる。認証許可／認証不許可を指示されたスレーブ50は、指示に従った処理を行う。

[0040] なお、認証許可／認証不許可を判断するためには、ユーザが、マスタ40の装置情報を入手しておく必要がある。マスタ40の装置情報は、スレーブ50の表示部23を確

認するユーザ自らが直接入手してもよいし、マスタ40を管理する他のユーザから通知してもらうようにしてもよい。また、入手のタイミングは、スレーブ50の表示部23に情報が表示された時であってもよいし、その表示よりも前であってもよい。

[0041] 表示部23の画面に表示されている装置情報が正しいとユーザに判断されて認証許可が指示された場合、スレーブ50は、マスタ40の公開鍵で暗号化された自己の公開鍵と乱数とを含む鍵生成要求を作成し、マスタ40へ送信する(ステップS1115)。図12Cは、鍵生成要求の一例を示す図である。マスタ40は、鍵生成要求を受信すると(ステップS1103)、スレーブ50の公開鍵で暗号化された乱数を含む鍵生成応答を、スレーブ50へ送信する(ステップS1104)。図12Dは、鍵生成応答の一例を示す図である。この鍵生成応答は、スレーブ50で受信される(ステップS1116)。その後、マスタ40及びスレーブ50は、マスタ40の公開鍵(PubKeyM)、スレーブ50の公開鍵(PubKeyS)、マスタ40のID(IDm)、スレーブ50のID(IDs)、スレーブ50が生成した乱数(Ns)及びマスタ40が生成した乱数(Nm)に基づいて、通信用の共通暗号鍵をそれぞれ生成する(ステップS1105、S1117)。通信用の共通暗号鍵は、例えば以下の式で生成される。

共通暗号鍵 = prf(PreMasterKey, PubKeyS||PubKeyM||IDm||IDs||Ns||Nm)

[0042] 一方、表示部23の画面に表示されている装置情報が誤っているとユーザに判断されて認証不許可が指示された場合、スレーブ50は、認証処理を終了する。なお、スレーブ50は、表示部23に表示してから所定時間内にユーザから入力がなければ、認証不許可と判断するようにしてもよい。

[0043] (2)三者間で行われる認証手順(図13)

これは、スレーブ50から送信される認証要求が、第1のマスタ40と第2のマスタ40とで受信されるケースである。この場合、スレーブ50は、第1のマスタ40及び第2のマスタ40からそれぞれ認証応答を受信して、2つの装置情報を表示部23の画面に表示させる。表示部23の画面表示例は、図7に示した通りである。ユーザは、表示部23の画面に表示されている2つの装置情報を目視確認し、入力部24を介して認証許可又は認証不許可を判断してスレーブ50に指示する。もちろん、ユーザは、認証許可すべきマスタ40の装置情報を知っているので、その装置情報を送信してきたマスタ4

0を選択して、認証許可を行う。なお、表示部23の画面に表示された何れの装置情報も既知の装置情報と一致しなければ、ユーザは、認証不許可を判断する。

なお、上述した認証処理は、四者間以上で行われる場合も同様である。また、鍵に代えて電子署名を装置情報に用いても同様に行われる。

[0044] (3)二者の間に不正者が割り込む場合の認証手順(図14)

スレーブ50は、認証要求をマスタ40に送信する。マスタ40は、認証要求に対して装置情報[ID1、鍵1]を含む認証応答をスレーブ40に送信する。しかし、この認証応答は、スレーブ50へ届かずに不正者装置90に受信される。不正者装置90は、マスタになりすますために、装置情報[ID1、鍵1]を偽装置情報[ID1、鍵2]に付け替えた認証応答を、スレーブ50に送信する。スレーブ50は、認証応答を受信し、その認証応答に含まれる装置情報を表示部23の画面に表示させる。ユーザは、表示部23の画面に表示されている装置情報を目視確認し、表示されている装置情報のうち、公開鍵情報が認証許可すべきマスタ40の装置情報と一致しないことを判断する。すなわち、ユーザは、表示された装置情報[ID1、鍵2]が、入手していたマスタ40の装置情報である[ID1、鍵1]と異なることを認識する。これに応じて、ユーザは、認証処理を終了する。なお、鍵に代えて電子署名を装置情報に用いても同様に行われる。

[0045] 以上のように、本発明の第2の実施形態に係る通信装置によれば、認証応答してきたマスタの装置情報をスレーブ側で画面表示させる。これにより、ユーザが、認証応答を送信してきた通信装置が認証許可すべきマスタであるか否かを、容易に判断することが可能となる。従って、認証処理の安全性及び確実性をさらに向上させることができる。

また、画面で確認された装置情報(ID)を用いて共通暗号鍵を生成すれば、実通信における秘匿性をさらに向上させることができる。

[0046] (第3の実施形態)

次に、上記第1の実施形態で説明したマスタ10及びスレーブ20について、具体的な構成及び認証の一例を説明する。なお、この第3の実施形態では、マスタをAPと、スレーブをクライアントとして記述する。図15は、認証部12及び22の詳細な構成例を示す図である。図15において、認証部12及び22は、公開鍵・秘密鍵生成部111

と、電子署名部112と、暗号化部113と、復号部114と、擬似乱数発生部115と、ハッシュ関数部116と、共通暗号鍵生成部117とを備える。もちろん、以下に説明する具体的な構成及び認証の例が、第2の実施形態で説明したマスタ40とスレーブ50とについても同様に適用可能であることは、言うまでもない。

[0047] 公開鍵・秘密鍵生成部111は、自己の公開鍵・秘密鍵ペアを生成する。この生成は、機器が起動される際又はその後自己の公開鍵・秘密鍵ペアの再生成が必要な際に行われる。公開鍵は公開される鍵であり、秘密鍵は公開されない鍵である。電子署名部112は、ハッシュ関数部116を用いて、メッセージを固定長に短縮し、秘密鍵と暗号化部113のアルゴリズムとで暗号化し、暗号化した結果を電子署名としてメッセージに付け加える。暗号化部113は、相手の公開鍵又は自己の秘密鍵又は相手と共有する共通暗号鍵を用いて暗号化するためのアルゴリズムを含む。復号部114は、自身の秘密鍵又は相手の公開鍵(電子署名の場合)又は相手と共有する共通暗号鍵を用いて復号するためのアルゴリズムを含む。擬似乱数発生部115は、規則性を予測しにくい擬似乱数生成機能を有し、ノンスや(必要な時)IDを生成する。このIDは、擬似乱数発生部115が発生する乱数であるが、第1の実施形態で説明した製品番号やMACアドレス等からなる識別番号と同じ役割を持つものであるため、同じ「ID」と表記する(本実施形態の具体例4を参照)。ハッシュ関数部116は、長いビット列を固定長のビット列に圧縮する一方向ハッシュ関数を含む。共通暗号鍵生成部117は、2つのノンス(乱数)に基づき、擬似乱数発生部115を用いて共通暗号鍵を生成する。

[0048] この公開鍵・秘密鍵生成部111、電子署名部112、暗号化部113、復号部114、擬似乱数発生部115、ハッシュ関数部116、及び共通暗号鍵生成部117は、図15のように認証部12及び22の内部モジュールとして実装してもよいし、個別的に認証部12及び22の外に置いて又は使用可能な外部共通モジュールを呼び出して使用するという形での実装してもよい。

以下、図16～図24を用いて、第3の実施形態におけるクライアントをAPに接続する際の認証及び鍵生成に関する手順について説明する。

[0049] (具体例1)

プローブ要求1600及びプローブ応答1601は、IEEE802．11で代表されるような従来標準のフォーマットを採用する。プローブ確認1602は、従来標準にはなく、本発明の接続方式を行うこととそれに必要なパラメータを知らせる機能を持つ新しいメッセージタイプである。認証要求1603以降のメッセージは、全て本発明規定の新しいフォーマットを採用する。認証要求1603のフォーマットの一例を図17に示す。HDRc1701は、クライアント20のアドレスやメッセージタイプを含むヘッダであり、従来の認証要求のヘッダと同様である。PLc1702は、従来と同様のペイロードである。PKc1704は、クライアント20の公開鍵である。IDc1703は、クライアント20のIDである。SIGNc1705は、ヘッダをはじめ全てのフィールドに対してクライアント20の電子署名部112を用いて署名したものである。クライアント20の送受信部21は、公開鍵・秘密鍵生成部111からクライアント20の公開鍵PKc1704を取得する。また、電子署名部112からSIGNc1705を取得し、認証部22が保持するIDc1703と合わせて認証要求1603を生成する。認証要求1603によって、クライアント20の公開鍵PKc1704をAP10に渡すことができる。

[0050] AP10が認証要求1603を受信すると、AP10の送受信部11は、認証要求1603に含まれるクライアント20の公開鍵PKc1704及び電子署名SIGNc1705を取り出し、AP10の認証部12に渡す。認証部12は、クライアント20の公開鍵PKc1704とAP10の復号部114とを用いてSIGNc1705を復号した結果を、受信した認証要求1603に対してAP10のハッシュ関数部116で自身のハッシュ関数を用いて、クライアント20の署名時に使用した同じハッシュ関数を掛けた結果と比較する(すなわち、完全性チェックを行う)。そして、認証部12は、結果が一致したら、受信した認証要求1603に含まれたID、すなわちIDcと、AP10の送受信部11で受信に使用された無線チャンネルの情報をAP10の表示部13に表示する。ユーザが、AP10の表示部13に表示されているIDc及び無線チャンネル情報が、認証すべきクライアントのIDc及び無線チャンネル情報と一致するか否かを確認し、一致したらAP10の入力部14を用いて認証許可を行う。

[0051] なお、本実施形態では、電子署名SIGNc1705を復号し、完全性を確認できた場合に、受信した認証要求1603に含まれたIDcと、送受信部11で受信に使用された

無線チャンネルの情報とをAP10の表示部13に表示しているが、電子署名を使用せず、受信した認証要求1603の内容を無条件に表示し、一致を確認してもよい。

[0052] 認証要求1603が成功した場合、AP10からクライアント20へ認証応答1605を返信する。認証応答1605のフォーマットの一例を図18に示す。PLa1802は、認証結果を含む。PKa1804は、AP10の公開鍵である。IDa1803は、AP10のIDである。SIGNa1805は、AP10の秘密鍵と電子署名とを用いた認証応答1605の各フィールドに対する署名である。AP10の送受信部11は、公開鍵・秘密鍵生成部111からクライアント20の公開鍵PKa1804を取得する。また、電子署名部112からSIGNa1805を取得し、認証部21が保持するIDa1803と合わせて認証応答1605を生成する。認証応答1605によって、AP10の公開鍵PKaをクライアント20に渡すことができる。

[0053] AP10が認証応答1605を送信した後、所定の全ての無線チャンネルのいずれかから、第三者装置が同じIDaを含んだ認証応答1605メッセージを発信しているか否かを監視する。このような発信があった場合、改竄・転送が行われたと判断する。

[0054] クライアント20が認証応答1605を受信すると、クライアント20の送受信部21は、認証応答1605に含まれるAP10の公開鍵PKa1804及び電子署名SIGNa1805を取り出し、クライアント20の認証部22に渡す。そして、AP10と同様の方法でメッセージの完全性をチェックする。これにより認証成功となる。

[0055] (具体例2)

認証要求メッセージが第三者装置に改竄・転送されることに対する監視を、クライアント20又はAP10が行う。第三者装置の送信したメッセージ全てをクライアント20が受信できる状況にある場合には、クライアント20が監視を行うのが有効である。クライアント20の送信したメッセージと第三者装置の送信したメッセージ全てをAP10が受信できる状況にある場合には、AP10が監視を行うのが有効である。クライアント20が監視を行う場合は、AP10からの認証応答が返信されるまでに受信した第三者装置の改竄した認証要求は、含まれた公開鍵と署名とを除いて自身が送出した認証要求と同じであれば、第三者装置の改竄・転送行為を断定する。AP10が監視を行う場合は、一定時間内に公開鍵と署名とを除いて全く同じ認証要求を2つ受信すれば、第

三者装置の改竄・転送行為を断定する。AP10が図19に示すような認証応答402を受信したら、公開鍵PKm1904と署名SIGNm1905を除いて同じ認証応答を2つ受信しているか、クライアント20も自身が送信した認証要求の公開鍵と署名とを改竄されたこの認証要求を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

[0056] 認証応答メッセージが第三者装置に改竄・転送されることに対する監視・断定は、認証要求メッセージと同じような処理の仕方を用い、クライアント20とAP10と役割を交換すればよい。クライアント20が図20に示すような認証応答404を受信したら、公開鍵PKm2004と署名SIGNm2005とを除いて同じ認証応答を2つ受信しているか、AP10も自身が送信した認証応答の公開鍵と署名とを改竄されたこの認証応答を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

[0057] (具体例3)

認証応答1605は、図21に示すようなフォーマットを一例として採用する。AP10の暗号化部113が、認証応答情報PLa2102、AP10の公開鍵PKa2104、AP10のIDa2103を、認証要求1603で受け取ったクライアント20の公開鍵PKcで暗号化して、認証応答1605をクライアント20に送信する。このような認証応答1605は、公開鍵PKcのペアである秘密鍵を持つクライアント20しか復号できない。

[0058] なお、この場合は、認証要求を行う段階で第三者装置の改竄はないと確認できたので、クライアント20又はAP10が図22に示すような認証応答404を受信することはない。第三者装置がこの段階からこのような認証応答を使用して攻撃しても、クライアント20にただ無視され、悪影響にはならない。

[0059] (具体例4)

クライアント20又はAP10のIDとして、クライアント接続を行う都度にクライアント20及びAP10の擬似乱数発生部115で生成した乱数を使用する。これは、MACアドレスや製品の型番より、さらに高い秘密性を持つ。ユーザ定義の名前をIDとしてここで使うことも可能であるが、事前に入力しておく手間がかかり、かつ、ユーザはなるべくユニーク(特に隣家の同様な機器と異なるよう)な名前を設定しなければならない。乱数を使用することで、次回接続時には違うIDになるので、盗まれても問題はない。

[0060] （具体例5）

認証に成功した場合、クライアント20は、AP10へ図23に示すような共通暗号鍵生成要求1606を送信する。共通暗号鍵生成要求1606は、ヘッダHDRc2301を除いた部分がクライアント20の暗号化部113においてAP10の公開鍵PKaを用いて暗号化される。IDc2302は、クライアント20のIDである。Nc2303は、クライアント20が生成した乱数（ノンス）である。クライアント20の暗号化部113は、クライアント20の送受信部21が保持するIDcと、クライアント20の擬似乱数発生部115が生成した乱数Ncを取得し、暗号化する。クライアント20の送受信部21は、暗号化されたIDcと、乱数NcにヘッダHDRc2301を付加し、共通暗号鍵生成要求1606を送信する。AP10の送受信部11が、共通暗号鍵生成要求1606を受信し、復号の対象となるデータを取り出して復号部114に渡す。復号部114において、自身の秘密鍵で復号する。復号結果において、IDは先に認証したクライアント20のIDcであることを確認する。確認できたら、復号結果で得られた乱数Ncを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通暗号鍵生成要求1606を廃棄し、鍵生成を中止とする。

[0061] AP10が、共通暗号鍵生成要求1606を正確に受信しかつ確認できた場合には、クライアント20に、図24に示す共通暗号鍵生成応答1607を返信する。共通暗号鍵生成応答1607は、ヘッダHDRa2401を除いた部分がクライアント20の公開鍵PKcを用いて暗号化される。IDa2402は、AP10のIDである。Na2403は、AP10が生成した乱数である。AP10の暗号化部113は、AP10の送受信部11が保持するIDaと、AP10の擬似乱数発生部115が生成した乱数Naを取得し、暗号化する。AP10の送受信部11は、暗号化されたIDaと乱数NaにヘッダHDRa2401を付加し、共通暗号鍵生成応答1607を送信する。クライアント20の送受信部21が、共通暗号鍵生成応答1607を受信し、復号の対象となるデータを取り出して復号部114に渡す。復号部114において、自身の秘密鍵で復号する。復号結果において、IDは先に認証したAP10のIDaであることを確認する。確認できたら、復号結果で得られたNaを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通暗号鍵生成応答1607を廃棄し、鍵生成を中止とする。

[0062] AP10及びクライアント20の共通暗号鍵生成部117において、ID又はMACアドレ

ス、及び乱数に基づいて、共有する共通鍵の生成が行われる。これで、AP10とクライアント20は、同じ鍵を生成して共有することになる。クライアント20とAP10とが生成した共通暗号鍵を、次のアソシエーションの作成に用いる。つまり、図16のアソシエーション要求1608及びアソシエーション応答1609も、この鍵を用いて暗号化される。一方、受信側は、この鍵を用いて受信したメッセージを復号する。なお、生成した鍵は、クライアント20とAP10との間のコントロールメッセージの送受信に用いるが、データ送受信のために別の鍵を用いてもよい。

[0063] また、プローブ要求／応答の前に、AP10及びクライアント20の双方において、その後の認証に使用する同じ暗号鍵を選択する動作が行われてもよい。この場合、この選択された暗号鍵を用いて、AP10からクライアント20へのチャレンジ指示、及びクライアント20からAP10へのチャレンジを暗号化した認証要求が行われる(図25)。

[0064] なお、IDは、通常は固定番号を使用するが、乱数をIDとして用いることも可能である。固定番号は、予めクライアント20に割り振られているものでもよいが、クライアント20毎にユーザが独自に設定しても構わない。このIDの設定は入力部24を介して行えば容易である。

[0065] また、AP10の上位装置としてルータ又はホームゲートウエイを有したシステムに適用することも可能である(図26)。この場合には、AP10が備えていた表示部13及び入力部14をルータ又はホームゲートウエイに備えさせて、AP10と同様の処理をルータ又はホームゲートウエイに行わせればよい。このシステム構成にすれば、AP10に認証機能を備えておく必要がなくなりAP10の構成が簡単になる。但し、この場合には、ルータ又はホームゲートウエイは、AP10とセキュアな通信経路で繋がれており、アクセスポイントは中継機能を果たす。なお、本発明は、ルータ或いはホームゲートウエイとアクセスポイントとの間に無線LANで繋ぐ場合の接続にも応用できる。

[0066] (関連する他の実施形態)

ネットワーク内に複数のAPが存在する場合、クライアントが1つのAPから他のAP近くまで移動した場合、他のAPとの間で再接続を行う必要がでてくる。この再接続においては、あらためて認証を行うか行わないかの2通りが考えられる。認証を行う場合、上記各実施形態の何れかの手順を実行して新規にクライアントの認証が行われる

ので、複数のAP間で認証済みのクライアントに関する情報交換をしておく必要がない。これに対して、認証を行わない場合、前の認証を再利用する必要があり、APの間でクライアントの認証結果に関する情報交換をする必要がある。過去の認証を再利用する場合、過去の認証情報を何処に保存するか、どのように再利用するかによって、以下のようにいくつかの実施形態が考えられる。

[0067] まず、クライアントのID情報の共有方式には、認証したクライアントの全ID情報を全APの間で共有するAP共有方式、APが自身で認証したクライアントのID情報のみを自身で管理し、AP全体でクライアントの全IDを分散的に共有するAP分散管理方式、及び認証済みのクライアントの全ID情報をルータに保存共有するルータ共有方式がある。

[0068] AP共有方式では、図27に示すように、認証応答(成功)2700によってAP10でのクライアント20に対する認証が成功すると、AP10は、認証済みのクライアント20のIDをのせたクライアントアナウンス2701を、ネットワーク内の全APaへマルチキャストする。クライアントアナウンス2701を受け取った各APaは、AP10へ応答2702を返信してもよいが返信しなくてもよい。AP10は、自身が認証したクライアント20のIDを認証済みID情報として保有すると共に、他のAPからも認証済みのIDがマルチキャスト電文により通知され、そのIDを認証済みID情報として保有する。従って、全APは、それぞれの内部に、認証済みの全ID情報を同じように保有することになる。その後、図28に示すように、複数のAPaの内の何れかのAPbが、クライアント20から認証要求2800を受信すると、APbは、クライアント20の認証済みID情報を自分が保有しているかどうかを調べる。APbは、クライアント20の認証済みID情報を保有していれば、認証済み処理手順として、認証応答(成功)2801をクライアント20へ返信する。保有していなければ、クライアント20に対して初回認証と見なして、上記第1～第3の実施形態で説明した通常の認証手順の何れかを実行する。

[0069] AP分散管理方式では、APはクライアントに対し認証を終えた後、このクライアントのID情報を他のAPへマルチキャストしない。図29に示したように、APbが、クライアント20から認証要求2900を受信した後、APbがクライアント20のID情報を認証済みID情報として持っていなければ、AP10を含め他のAPへ、クライアント20のID情報

をのせたアクセス要求(ID)2901をマルチキャストする。すなわち、他のAPに認証済みID情報を保有しているかどうかを問い合わせる。指定時間内に、クライアント20の元の接続先AP10からアクセス応答2902を返信されたら、APbは、認証済み処理手順として、認証応答(成功)2903をクライアント20へ送信する。どのAPからもアクセス応答がなければ、APbは、クライアント20からの認証要求2900が初回認証であると見なして通常の認証手順を実行する。

[0070] ルータ共有方式では、図30に示すとおり、AP10はクライアント20に対し認証を終えた後、クライアント20の認証済みID情報をのせたクライアントアナウンス3001をルータへ送信する。クライアントアナウンス3001を受信したルータは、自分のデータベースにクライアント20のIDを認証済みID情報として登録して、応答3002を返信する。その後、クライアント20が移動して別のAPであるAPbと認証を試みたときには、図31に示すように、APbは、認証要求3100に対して、クライアント20が自分のクライアントでないため、ルータへクライアント20のID情報をのせたアクセス要求(ID)3101を送信する。アクセス要求(ID)3101を受信したルータは、自分のデータベースを検索して、クライアント20の認証済みID情報の登録の有無を調べ、登録有りの場合、認証済み処理手順として、その結果をアクセス応答3102でAPbへ返信する。認証済みID情報の登録があれば、認証成功、無ければ認証不許可となる。アクセス応答3102の内容が認証成功であれば、APbは、クライアント20へ認証応答(成功)3103を送信する。アクセス応答3102の内容が認証不成功であれば、クライアント20に対して初回認証と見なして、APbはクライアント20との間で上記第1～第3の実施形態で説明した認証手順の何れかを実行する。

[0071] なお、AP共有方式及びAP分散管理方式では、APは互に信頼関係にあり、AP間はセキュアな通信手段を用いるものとする。また、ルータ共有方式では、APとルータとが互に信頼関係にあり、セキュアな通信手段を用いるものとする。

[0072] 一方、上記各実施形態において通信が終了した場合、ユーザがクライアントの設置を停止する場合、古い認証済みIDが残っていない方がよい。そこで、認証済みのID情報を削除する方法を以下に説明する。

[0073] クライアントをネットワークから永久に切り離すには、図32のように、クライアント20か

らAP10へ自身のIDを付けて切断電文3202を送る。切断電文を受信したAP10は、クライアント20のID情報を、手順3203により、自分のデータベースから削除する。このためには、クライアント20が、ユーザが接続切断を選択すると切断電文がAP1に送信され、ネットワーク内の装置が記憶している認証済みID情報からクライアント20のID情報を消去するようにすればよい。

[0074] AP10以外に他のAPが認証済みID情報を共有するAP共有方式やAP分散管理方式のような場合には、図33に示すように、切断電文3302を受信したAP10は、マルチキャストの切断電文3303により、消去すべき認証済みID情報をAPaに通知して消去を要求し、消去要求を受信したAPaは、消去すべき認証済みID情報を記憶している場合、そのID情報を消去する。最初に切断電文を受信したAP10でも、認証済みID情報にクライアント20のID情報を記憶している場合、手順3304において、消去する。APaは、認証済みID情報を消去の後、切断応答電文3306をAP10に返す。その後、AP10は、切断応答電文3307をクライアント20に返す。

[0075] 認証済みID情報をルータが保存するルータ共有方式では、図34のように、クライアント20が、最寄りのAPに切断電文3402に自身のID情報を付加して送信する。APは、切断電文3402を切断電文3403として、ルータに転送する。ルータは、受信したID情報が認証済みID情報かどうか確認し、認証済みの場合、手順3404において、そのID情報を消去する。その後、切断応答3405をAPに返信し、APは、切断応答3406として、クライアント20に転送する。

[0076] また、クライアントに対して切断処理をしないまま、電源を切断するなどして永久に切り離した場合には、ユーザは、AP又はルータに備えられている、そのクライアントのIDを直接削除する機能を利用するようにしてもよい。このためには、AP又はルータに、認証済みID情報を表示できる表示部と、表示された認証済みID情報の何れかを削除する操作部を設け、ネットワーク内の装置が記憶している認証済みID情報から所定又は所望のクライアントの認証を解除することができるようにすればよい。認証済みID情報を複数のアクセスポイントに記憶する方式の場合は、マルチキャストの消去要求電文により、消去すべき認証済みID情報を通知し、消去要求を受信したAPやルータは、前記消去すべき認証済みID情報を記憶している場合、消去するよう

にすればよい。

[0077] また、上記実施形態において、APが認証を行う場合、APが宅内の各所に複数設置してあると、ユーザはAPを設置してある場所に移動する必要がある。この場合、APの表示部の情報を表示部付の手元リモコン装置により見ることができるようにすれば、移動が不必要になる。リモコンとAPの間でセキュアな無線通信路を設定できるようにすればよい。リモコンはID情報を確認し、認証許可を指示するためだけの機能でよいので、暗号化などのない簡単な伝送路を適用してもよい。このためには、APの表示部と認証部をリモコン装置上に設け、APの本体とリモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにすればよい。ルータが認証を行うシステムの場合も、同様のリモコン構成とすれば、同様の作業を行うことができる。

[0078] リモコン装置をAPやルータの本体部に設けた接続部に挿入しておくと、リモコン装置と本体部分が直接結合できるようにしておき、認証処理を行う場合に、リモコン装置を本体部から取り出して、ユーザが移動できるようにしてもよい。リモコン装置を本体部から外すときに、本体部とリモコン装置の間でリモコン無線通信用の共有鍵Rを決めて、以降の認証処理中に行う表示用のID情報の送信、認証許可の入力操作情報の送信、暗号鍵選択のための暗号鍵番号の送信などの本体部とリモコン装置間の通信において、共有鍵Rを使用して送信データを暗号化、復号化すれば、第3者に送信データの内容を知られることがなくなる。共有鍵Rは、リモコン装置を本体部から外すたびに新たに決めるようにすることができ、セキュアな通信路となる。

[0079] リモコン装置を本体部から外すときに共有鍵Rを設定する方法は、種々考えられる。一例として、リモコン装置を本体部から外す際に、リモコン装置の移動を感知するスイッチを本体部に設けておき、スイッチが移動を感知すると、すぐさま新たな共有鍵Rを本体部がリモコン装置に供給するようにすればよい。リモコン装置を本体部に挿入してある状態で、定期的に共有鍵Rの値を変更するようにして、リモコン装置を外したときに、最新の共有鍵Rを使用できるようにしてもよい。共有鍵Rの変更は、リモコン装置と本体部とが有線接続状態で行えるので、共有鍵を盗まれる恐れは実質上ないといえる。

[0080] リモコン装置をユーザが放置する又は紛失する懸念があるので、一定時間以上リモ

コン装置が本体部から外されている場合、本体部とリモコン装置の何れか又は両方が警告音を発生するようにするとよい。認証作業ののちリモコン装置を本体部に再び挿入するまで、クライアントの通信アプリケーションを開始できないようにしてもよい。

産業上の利用可能性

[0081] 本発明は、通信装置間の認証接続を行う通信ネットワークシステム等に利用可能であり、特に認証処理におけるセキュリティの向上と設定の簡単化を両立させたい場合等に適している。

請求の範囲

[1] 他の通信装置から接続のための認証を要求される通信装置であって、

通信装置を一意に特定できる装置情報を含む認証要求を、前記他の通信装置から受信する受信部と、

前記認証要求に含まれる装置情報を画面に表示する表示部と、

前記表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、

前記入力部に入力された指示に従って、前記他の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備える、通信装置。

[2] 他の通信装置へ接続のための認証を要求する通信装置であって、

通信装置を一意に特定できる装置情報を含む認証要求を、前記他の通信装置へ送信する送信部と、

前記認証要求に対応した装置情報を含む認証応答を、前記他の通信装置から受信する受信部と、

前記認証応答に含まれる装置情報を画面に表示する表示部と、

前記表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、

前記入力部に入力された指示に従って、前記他の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備える、通信装置。

[3] 前記受信部が、複数の前記他の通信装置から複数の認証要求を受信した場合、前記表示部は、当該複数の認証要求に含まれる複数の装置情報を画面に同時に表示することを特徴とする、請求項1に記載の通信装置。

[4] 前記受信部が、複数の前記他の通信装置から複数の認証応答を受信した場合、前記表示部は、当該複数の認証応答に含まれる複数の装置情報を画面に同時に表示することを特徴とする、請求項2に記載の通信装置。

[5] 前記認証部は、所定時間の経過時に前記入力部へユーザ指示がなければ、前記他の通信装置を認証不許可にする処理を実行することを特徴とする、請求項1に記載の通信装置。

[6] 前記認証部は、所定時間の経過時に前記入力部へユーザ指示がなければ、前記他の通信装置を認証不許可にする処理を実行することを特徴とする、請求項2に記載の通信装置。

[7] 前記装置情報は、通信装置の識別番号、及び公開鍵又は電子署名の何れかが、少なくとも含まれることを特徴とする、請求項1に記載の通信装置。

[8] 前記装置情報は、通信装置の識別番号、及び公開鍵又は電子署名の何れかが、少なくとも含まれることを特徴とする、請求項2に記載の通信装置。

[9] 前記認証部は、前記他の通信装置から受信した認証要求に含まれる識別番号を用いて、共通暗号鍵を生成することを特徴とする、請求項7に記載の通信装置。

[10] 前記認証部は、前記他の通信装置から受信した認証応答に含まれる識別番号を用いて、共通暗号鍵を生成することを特徴とする、請求項8に記載の通信装置。

[11] 第1の通信装置を第2の通信装置に接続させるために認証処理を実行する通信システムであって、

前記第1の通信装置は、

通信装置を一意に特定できる装置情報を含む認証要求を、前記第2の通信装置へ送信する送信部と、

前記認証要求に対応した装置情報を含む認証応答を、前記第2の通信装置から受信する受信部と、

前記認証応答に従って、前記第2の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備え、

前記第2の通信装置は、

前記認証要求を前記第1の通信装置から受信する受信部と、

前記認証要求に含まれる装置情報を画面に表示する表示部と、

前記表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、

前記入力部に入力された指示に従って、前記第1の通信装置との認証許可又は認証不許可の処理を実行する認証部と、

前記認証部に従って、認証許可又は認証不許可を指示する前記認証応答を前

記第1の通信装置に送信する送信部とを備える、通信システム。

[12] 第1の通信装置を第2の通信装置に接続させるために認証処理を実行する通信システムであって、

前記第1の通信装置は、

通信装置を一意に特定できる装置情報を含む認証要求を、前記第2の通信装置へ送信する送信部と、

前記認証要求に対応した装置情報を含む認証応答を、前記第2の通信装置から受信する受信部と、

前記認証要求に含まれる装置情報を画面に表示する表示部と、

前記表示部の画面に基づいてユーザによって判断された指示を入力する入力部と、

前記入力部に入力された指示に従って、前記第2の通信装置との認証許可又は認証不許可の処理を実行する認証部とを備え、

前記第2の通信装置は、

前記認証要求を前記第1の通信装置から受信する受信部と、

前記認証要求に対応した装置情報を含む認証応答を作成する認証部と、

前記認証応答を前記第1の通信装置に送信する送信部とを備える、通信システム。

[13] 第1の通信装置を第2の通信装置に接続させるために認証処理を実行する認証方法であって、

前記第1の通信装置が、通信装置を一意に特定できる装置情報を含む認証要求を、前記第2の通信装置へ送信するステップ、

前記第2の通信装置が、前記認証要求を前記第1の通信装置から受信するステップ、

前記第2の通信装置が、前記認証要求に含まれる装置情報を画面に表示するステップ、

前記第2の通信装置が、前記表示された画面に基づいてユーザによって判断された指示を入力するステップ、

前記第2の通信装置が、前記入力された指示に従って、前記第1の通信装置との認証許可又は認証不許可の処理を実行するステップ、

前記第2の通信装置が、前記認証の処理に従って、認証許可又は認証不許可を指示する前記認証要求に対応した装置情報を含む認証応答を前記第1の通信装置に送信するステップ、

前記第1の通信装置が、前記認証応答を、前記第2の通信装置から受信するステップ、及び

前記第1の通信装置が、前記認証応答に従って、前記第2の通信装置との認証許可又は認証不許可の処理を実行するステップとを備える、認証方法。

[14] 第1の通信装置を第2の通信装置に接続させるために認証処理を実行する認証方法であって、

前記第1の通信装置が、通信装置を一意に特定できる装置情報を含む認証要求を、前記第2の通信装置へ送信するステップ、

前記第2の通信装置が、前記認証要求を前記第1の通信装置から受信するステップ、

前記第2の通信装置が、前記認証要求に対応した装置情報を含む認証応答を作成するステップ、

前記第2の通信装置が、前記認証応答を前記第1の通信装置に送信するステップ、

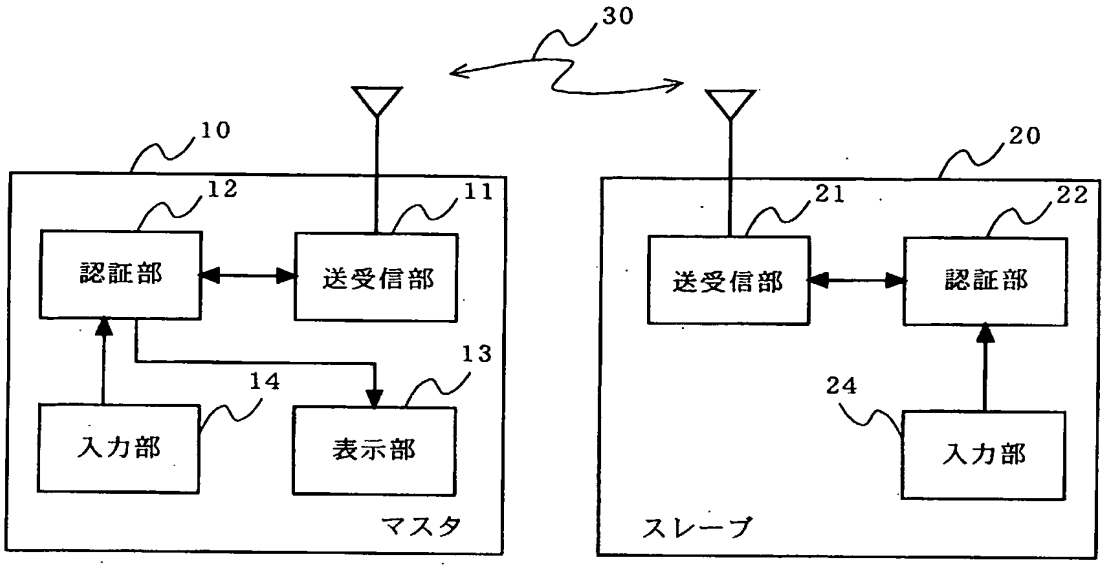
前記第1の通信装置が、前記認証要求に対応した装置情報を含む認証応答を、前記第2の通信装置から受信するステップ、

前記第1の通信装置が、前記認証要求に含まれる装置情報を画面に表示するステップ、

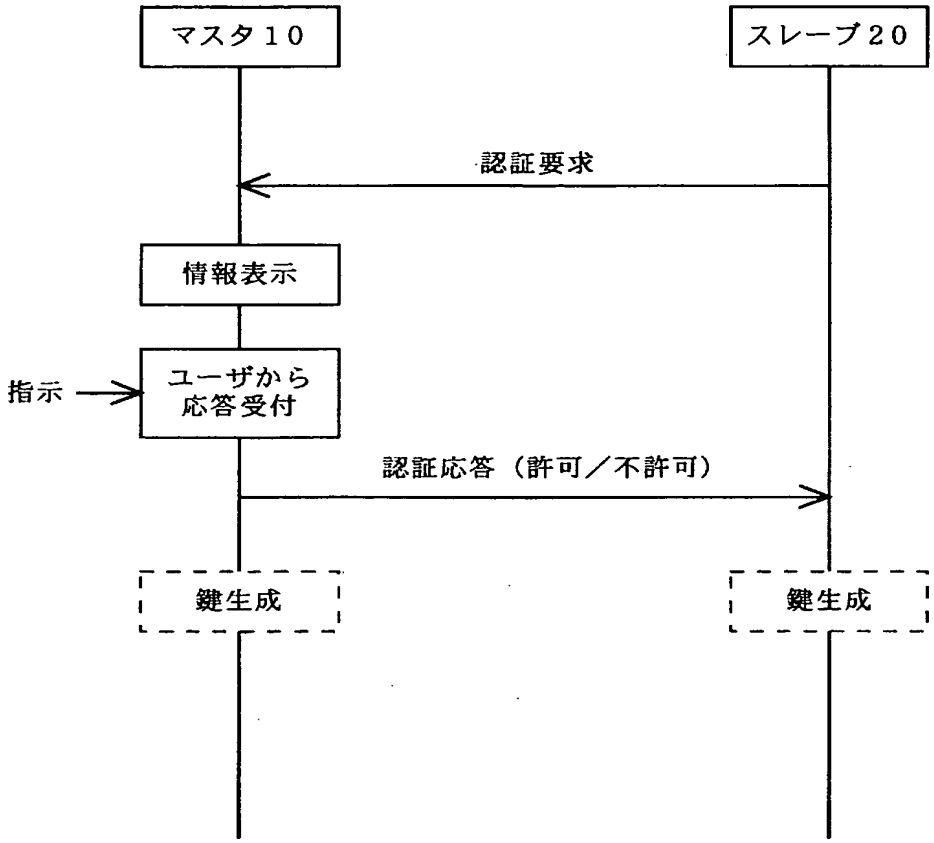
前記第1の通信装置が、前記表示された画面に基づいてユーザによって判断された指示を入力するステップ、及び

前記入力された指示に従って、前記第2の通信装置との認証許可又は認証不許可の処理を実行するステップとを備える、認証方法。

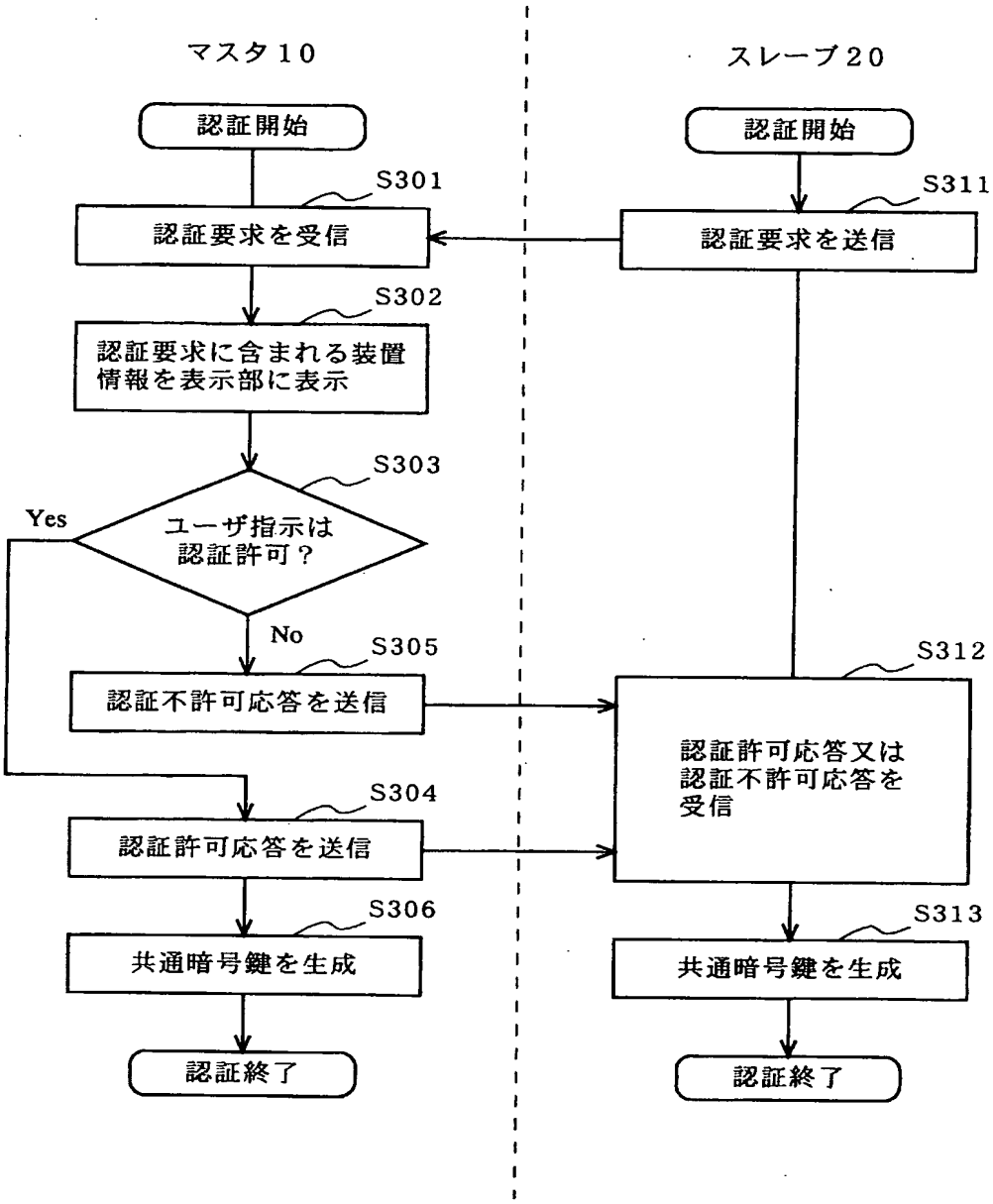
[図1]


30
10
12
11
認証部
送受信部
13
14
入力部
表示部
マスタ
20
21
22
送受信部
認証部
24
入力部
スレーブ

[図2]



[図3]


マスタ10
スレーブ20
認証開始
認証開始
S301
S311
認証要求を受信
認証要求を送信
S302
認証要求に含まれる装置情報を表示部に表示
S303
Yes
ユーザ指示は認証許可？
No
S305
S312
認証不許可応答を送信
認証許可応答又は認証不許可応答を受信
S304
認証許可応答を送信
S306
S313
共通暗号鍵を生成
共通暗号鍵を生成
認証終了
認証終了

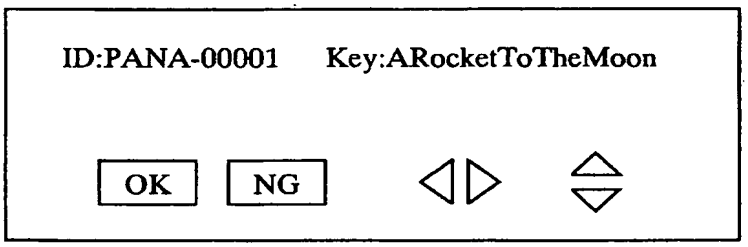
[図4A]

認証要求
識別番号（ＩＤｓ）
公開鍵（ＰｕｂＫｅｙ）
暗号方式（ＥｎｃＡｌｇ）
［電子署名（Ｓｉｇｎ）、電子署名方式（ＳｉｇＡｌｇ）］

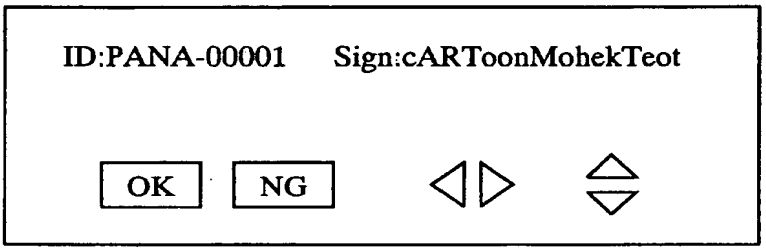
[図4B]

認証応答
識別番号（ＰｕｂＫｅｙ（ＩＤｍ））
乱数（ＰｕｂＫｅｙ（Ｎ））

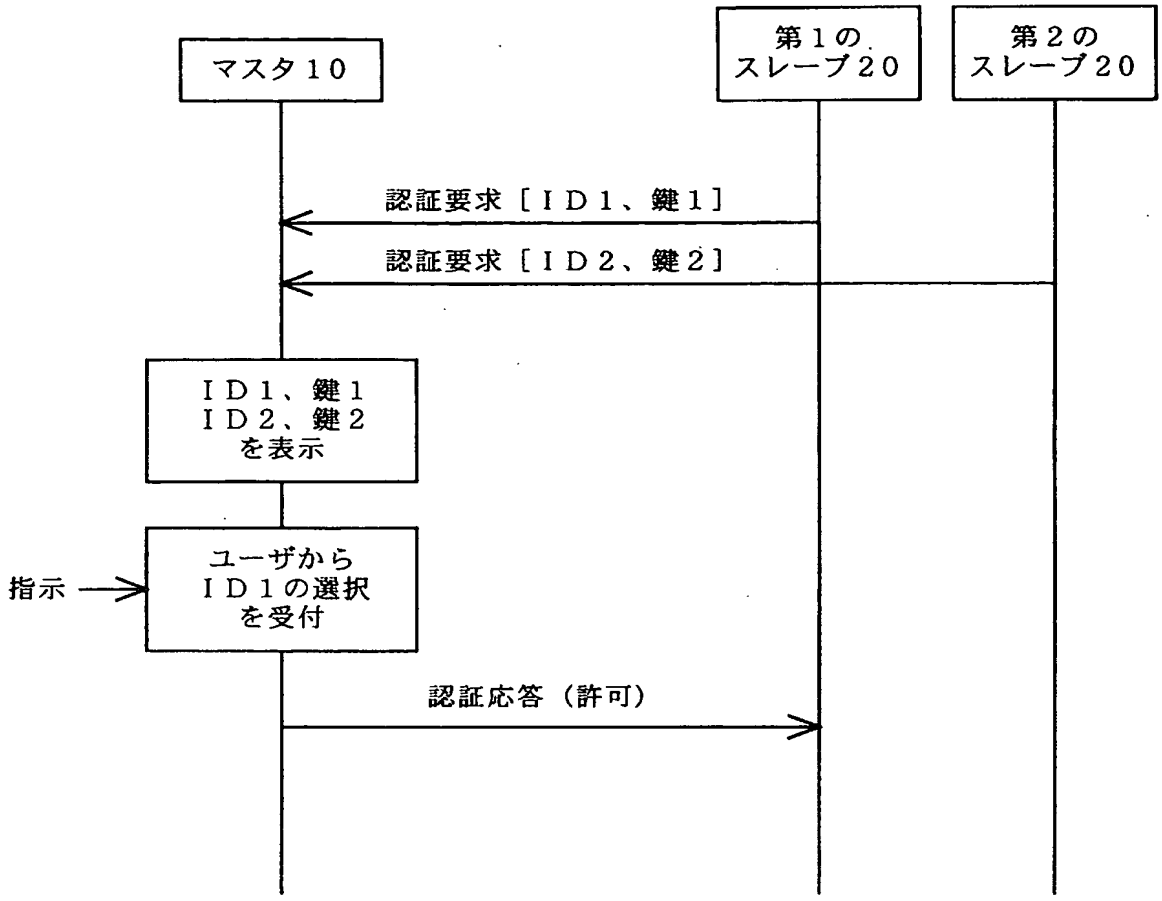
[図5A]


ID:PANA-00001 Key:ARocketToTheMoon
OK
NG

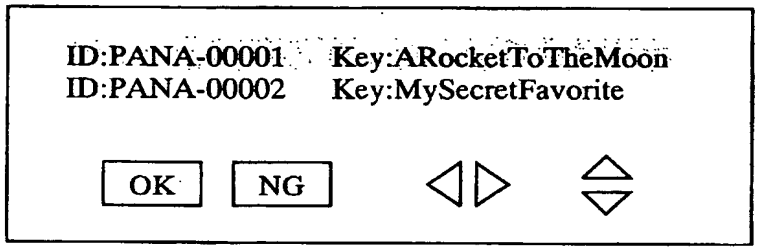
[図5B]


ID:PANA-00001 Sign:cARToonMohekTeot
OK
NG

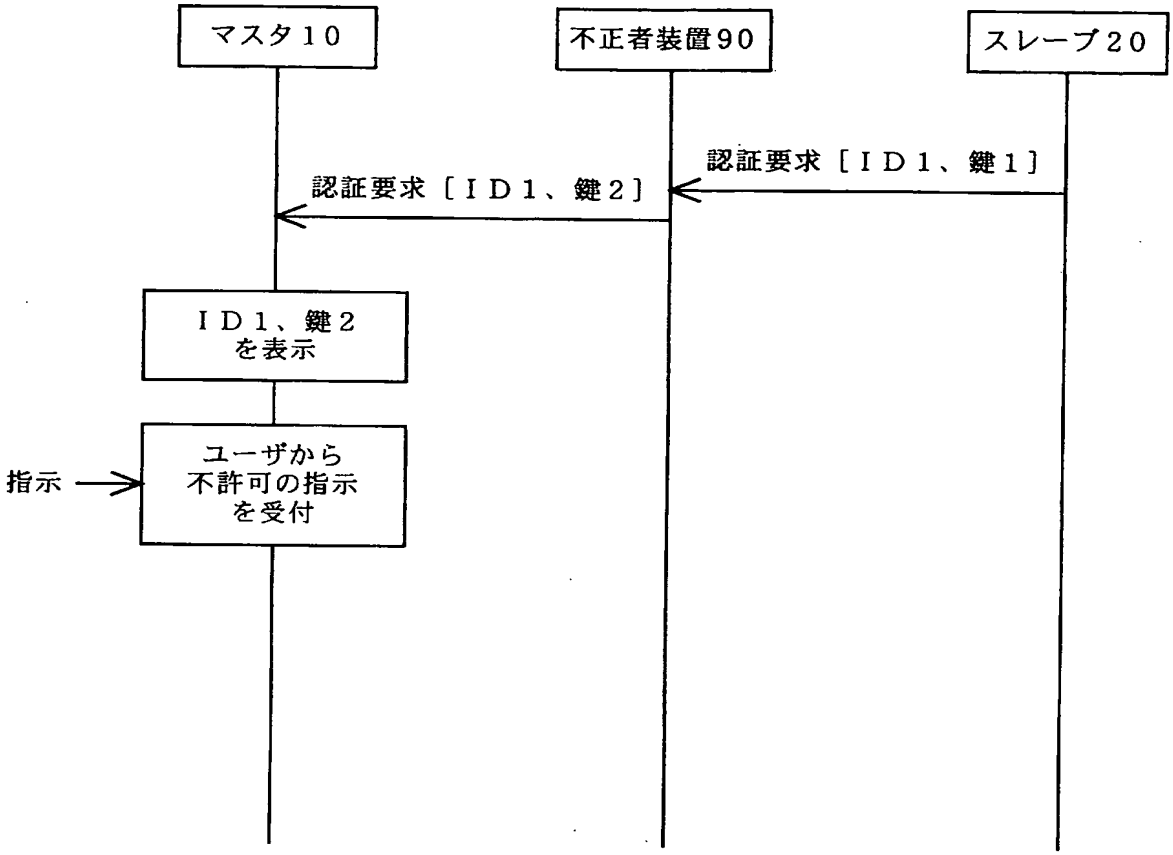
[図6]


マスタ１０
第１の
スレーブ２０
第２の
スレーブ２０
認証要求［ＩＤ１、鍵１］
認証要求［ＩＤ２、鍵２］
ＩＤ１、鍵１
ＩＤ２、鍵２
を表示
指示
ユーザから
ＩＤ１の選択
を受付
認証応答（許可）

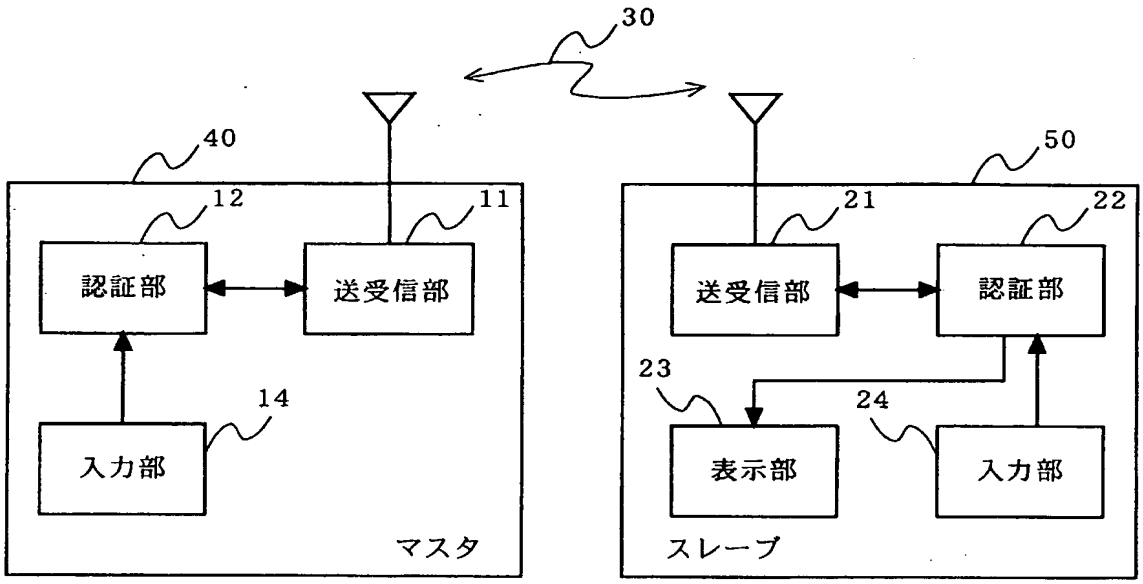
[図7]


ID:PANA-00001 Key:ARocketToTheMoon
ID:PANA-00002 Key:MySecretFavorite
OK
NG

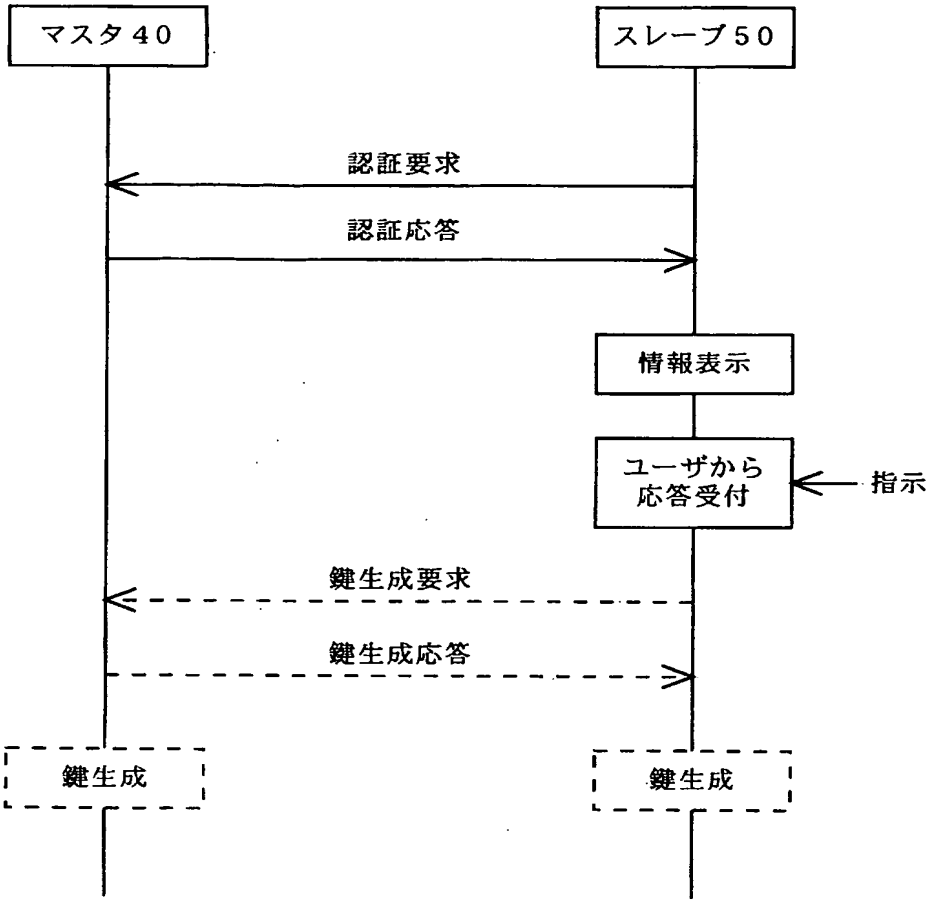
[図8]


マスタ10
不正者装置90
スレーブ20
認証要求［ＩＤ１、鍵１］
認証要求［ＩＤ１、鍵２］
ＩＤ１、鍵２
を表示
指示
ユーザから
不許可の指示
を受付

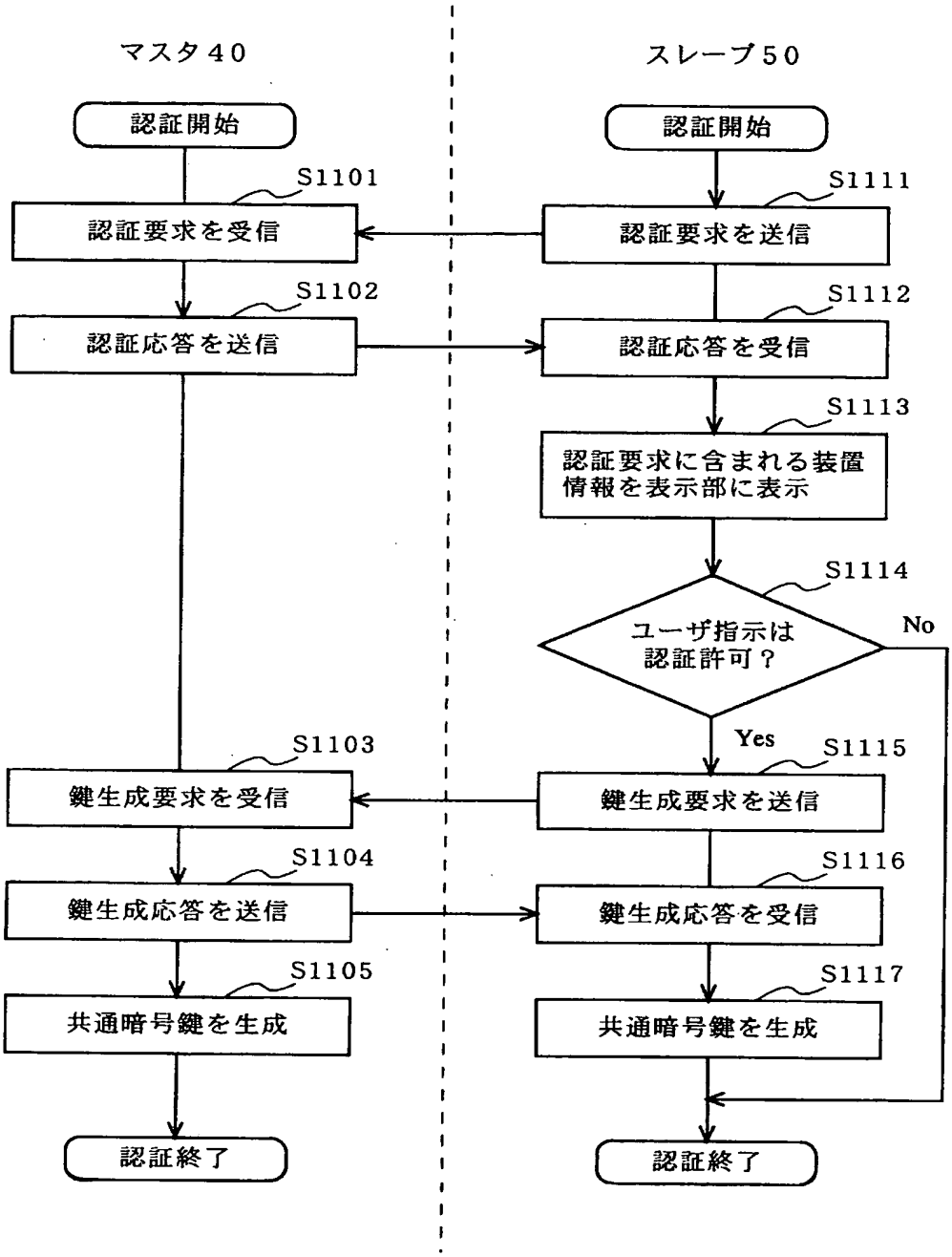
[図9]


30
40
50
12
11
21
22
認証部
送受信部
送受信部
認証部
23
24
14
表示部
入力部
入力部
マスタ
スレーブ

[図10]


マスタ４０
スレーブ５０
認証要求
認証応答
情報表示
ユーザから
応答受付
指示
鍵生成要求
鍵生成応答
鍵生成
鍵生成

[図11]


マスタ40
スレーブ50
認証開始
認証開始
S1101
認証要求を受信
S1111
認証要求を送信
S1102
認証応答を送信
S1112
認証応答を受信
S1113
認証要求に含まれる装置情報を表示部に表示
S1114
ユーザ指示は認証許可？
No
Yes
S1103
鍵生成要求を受信
S1115
鍵生成要求を送信
S1104
鍵生成応答を送信
S1116
鍵生成応答を受信
S1105
共通暗号鍵を生成
S1117
共通暗号鍵を生成
認証終了
認証終了

[図12A]

認証要求
識別番号（ＩＤｓ）

[図12B]

認証応答
識別番号（ＩＤｍ）
マスタの公開鍵（ＰｕｂＫｅｙＭ）
暗号方式（ＥｎｃＡｌｇ）
[電子署名（ＳｉｇｎＭ）、電子署名方式（ＳｉｇＡｌｇ）]

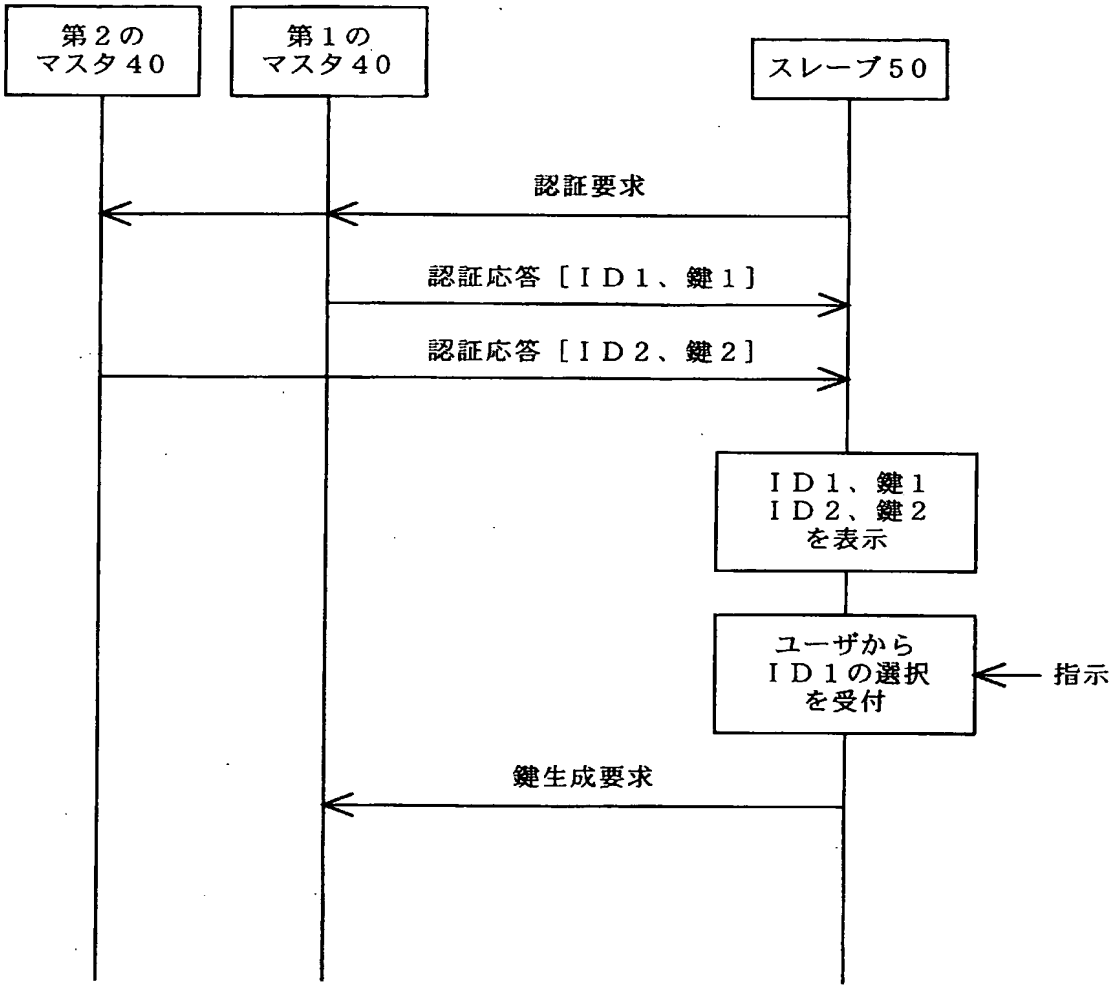
[図12C]

鍵生成要求
スレーブの公開鍵（ＰｕｂＫｅｙＭ（ＰｕｂＫｅｙＳ））
乱数１（ＰｕｂＫｅｙＭ（Ｎｓ））

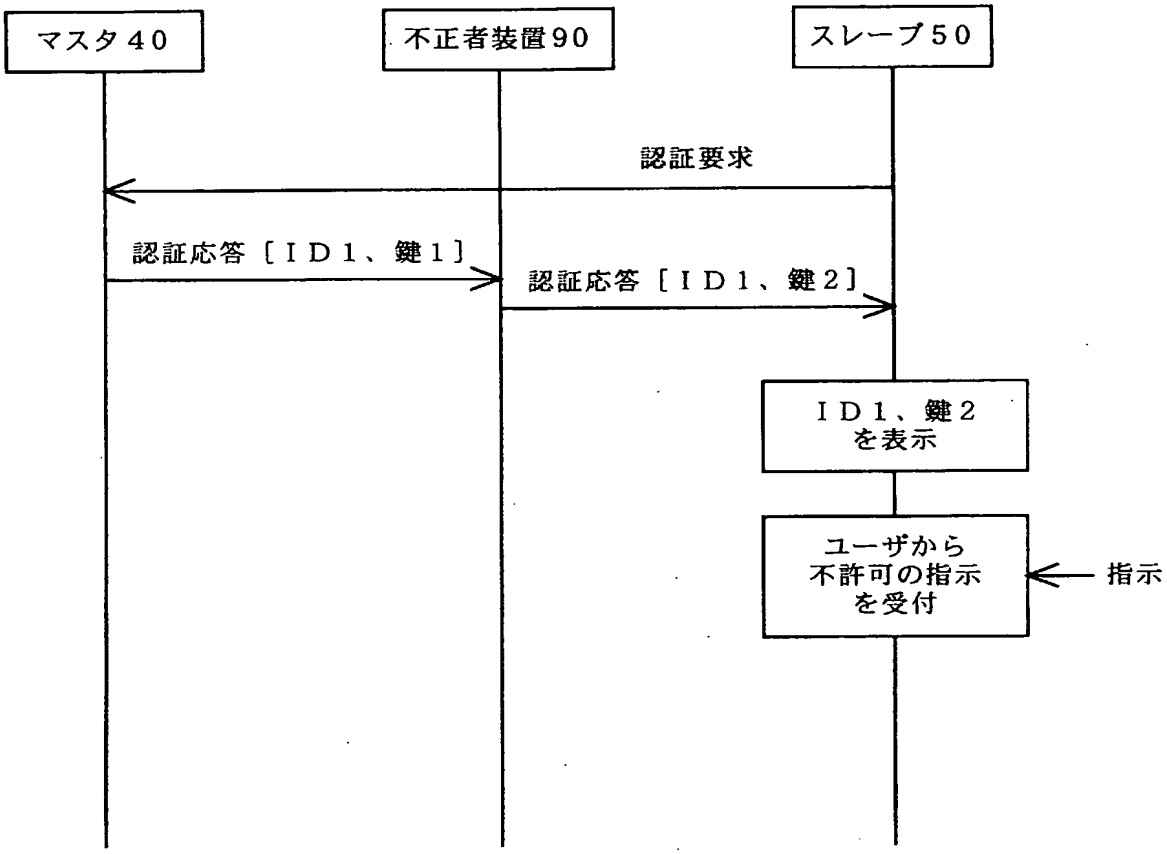
[図12D]

鍵生成応答
乱数２（ＰｕｂＫｅｙＳ（Ｎｍ））

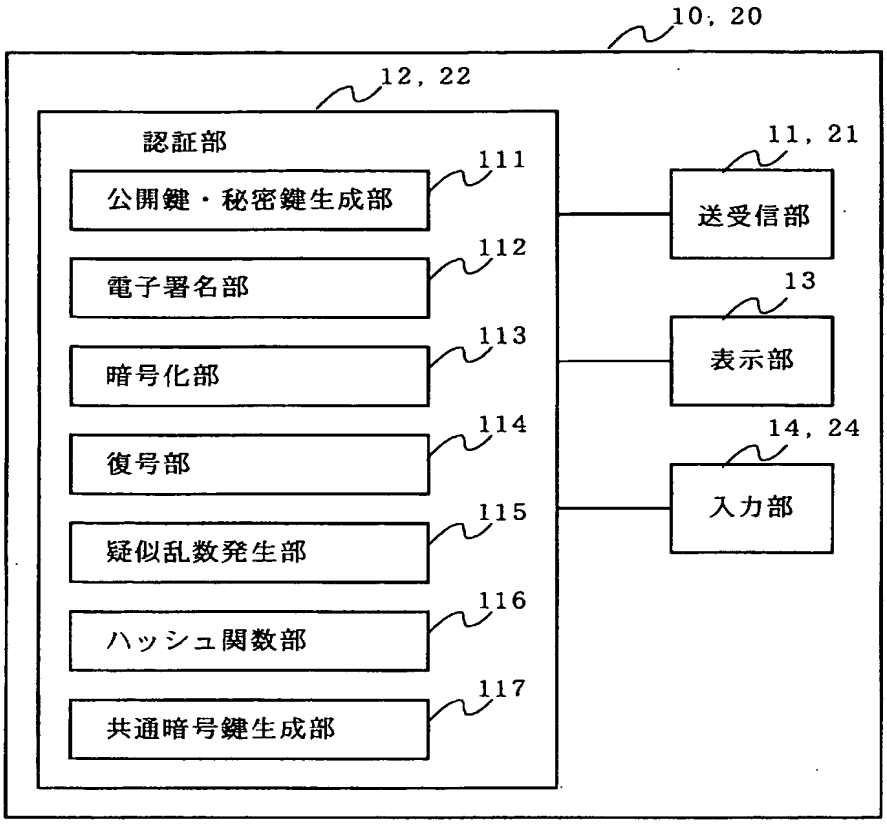
[図13]


第２の
マスタ４０
第１の
マスタ４０
スレーブ５０
認証要求
認証応答［ＩＤ１、鍵１］
認証応答［ＩＤ２、鍵２］
ＩＤ１、鍵１
ＩＤ２、鍵２
を表示
ユーザから
ＩＤ１の選択
を受付
指示
鍵生成要求

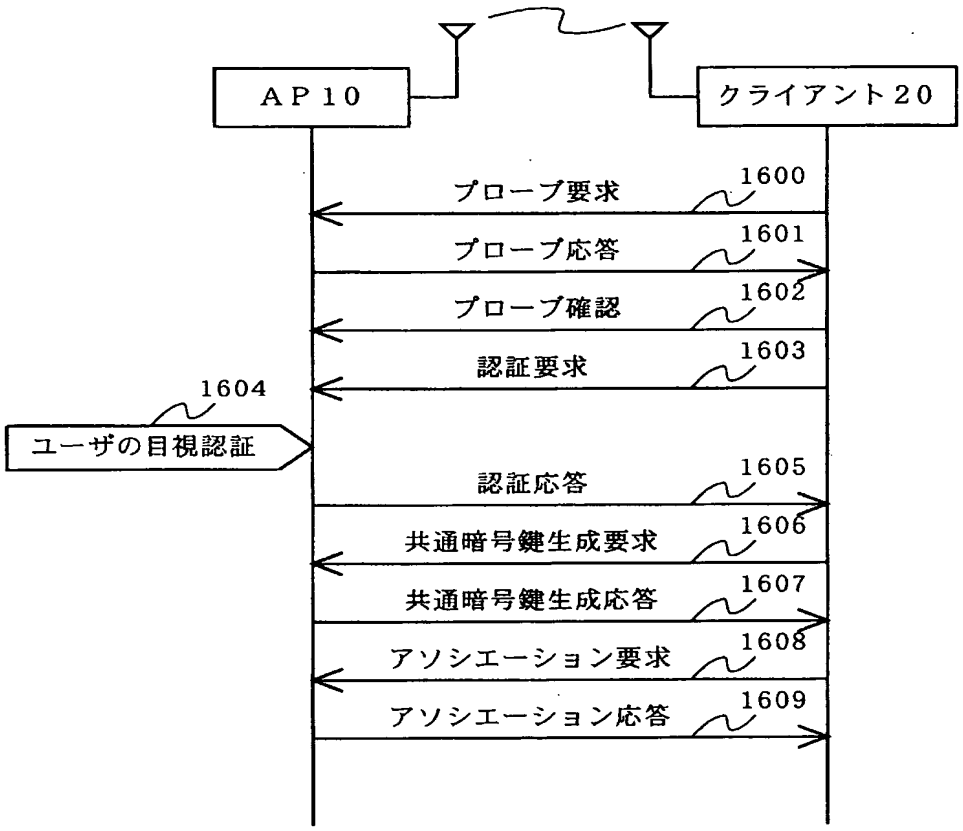
[図14]


マスタ４０
不正者装置９０
スレーブ５０
認証要求
認証応答［ＩＤ１、鍵１］
認証応答［ＩＤ１、鍵２］
ＩＤ１、鍵２
を表示
ユーザから
不許可の指示
を受付
指示

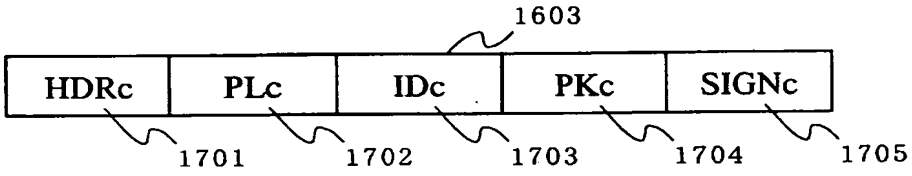
[図15]


10, 20
12, 22
認証部
111
公開鍵・秘密鍵生成部
112
電子署名部
113
暗号化部
114
復号部
115
疑似乱数発生部
116
ハッシュ関数部
117
共通暗号鍵生成部
11, 21
送受信部
13
表示部
14, 24
入力部

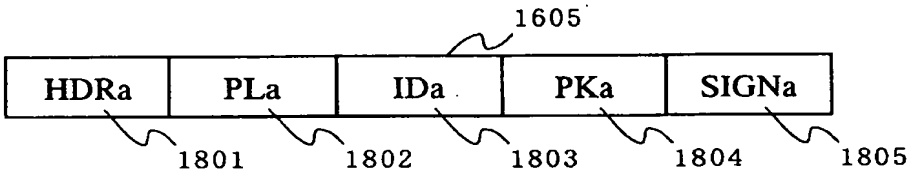
[図16]


AP10
クライアント20
プローブ要求
1600
プローブ応答
1601
プローブ確認
1602
認証要求
1603
1604
ユーザの目視認証
認証応答
1605
共通暗号鍵生成要求
1606
共通暗号鍵生成応答
1607
アソシエーション要求
1608
アソシエーション応答
1609

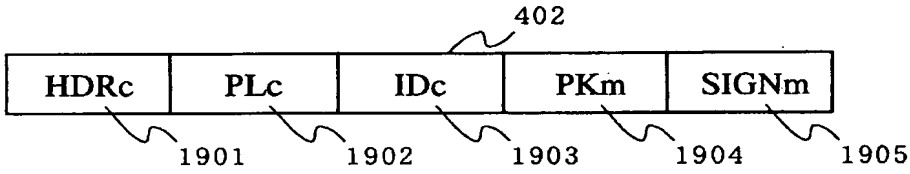
[図17]



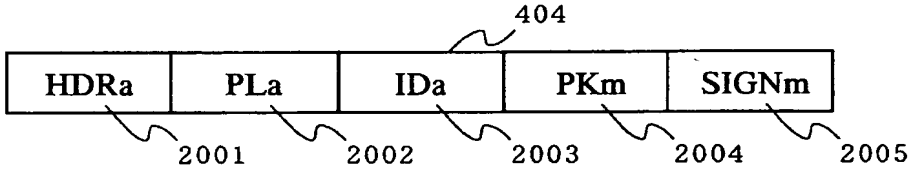
[図18]



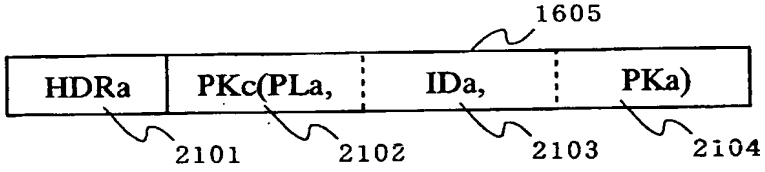
[図19]



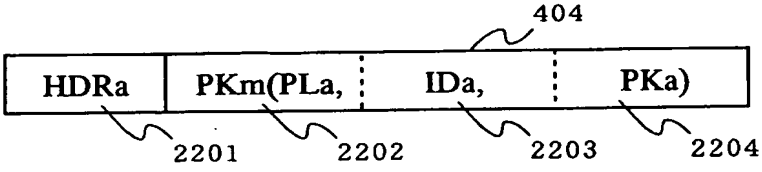
[図20]



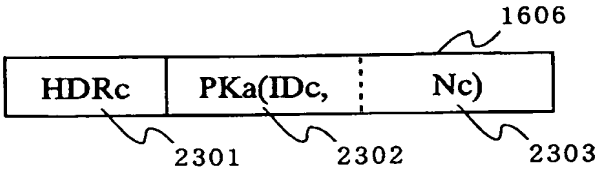
[図21]



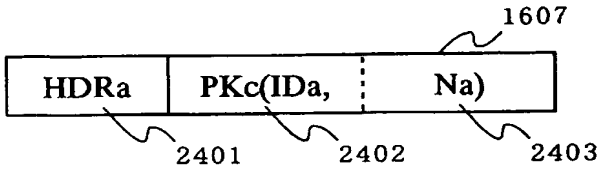
[図22]



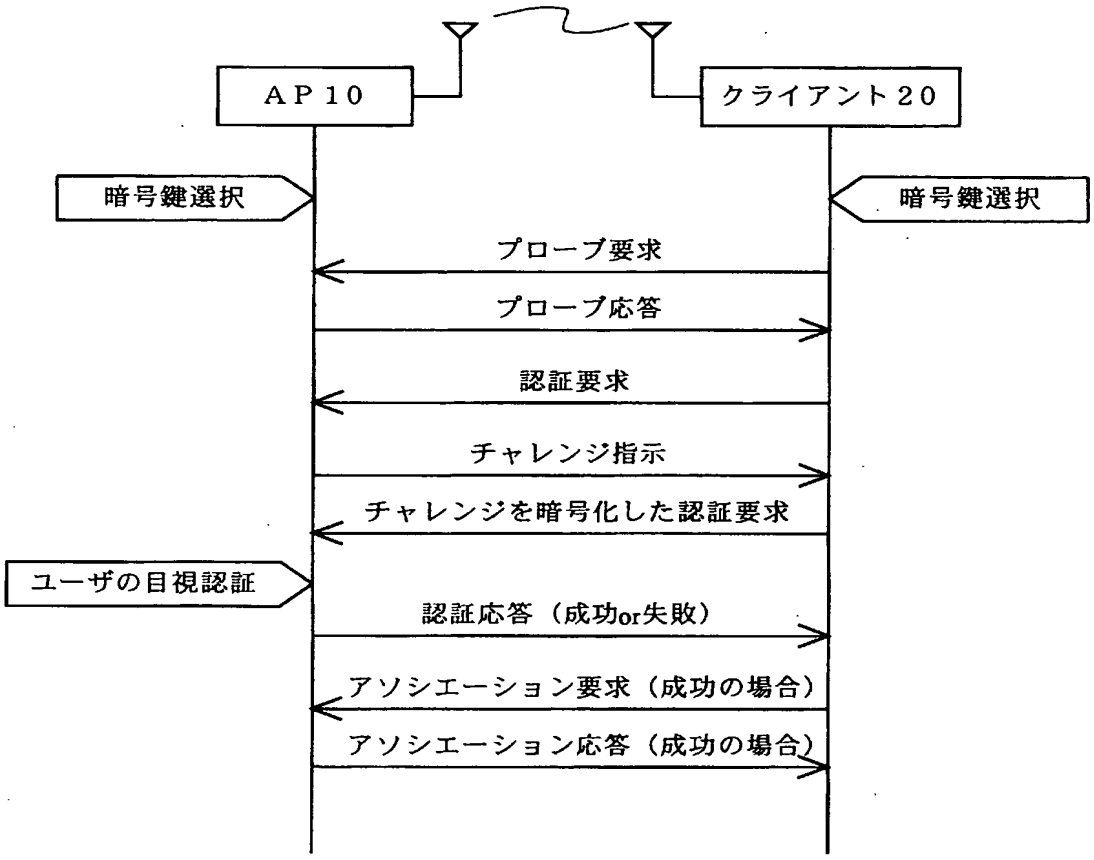
[図23]


1606
HDRc
PKa(IDc,
Nc)
2301
2302
2303

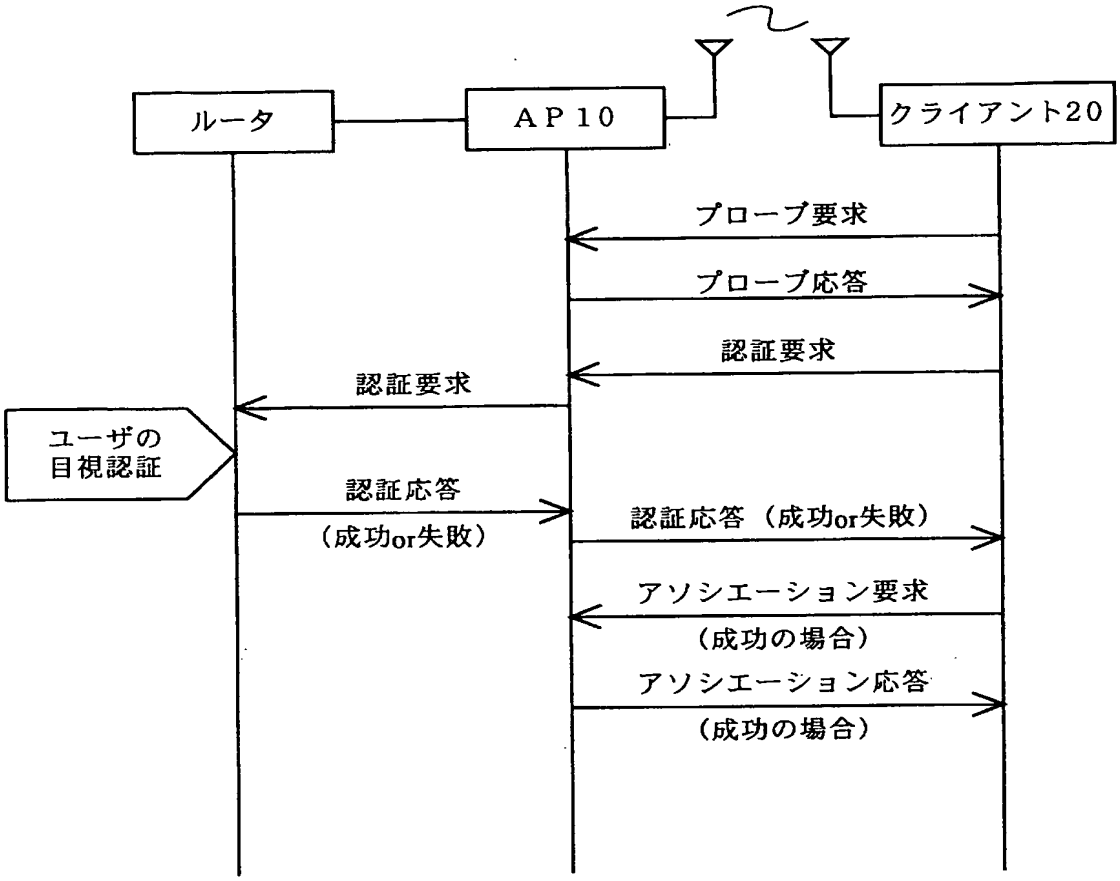
[図24]


1607
HDRa
PKc(IDa,
Na)
2401
2402
2403

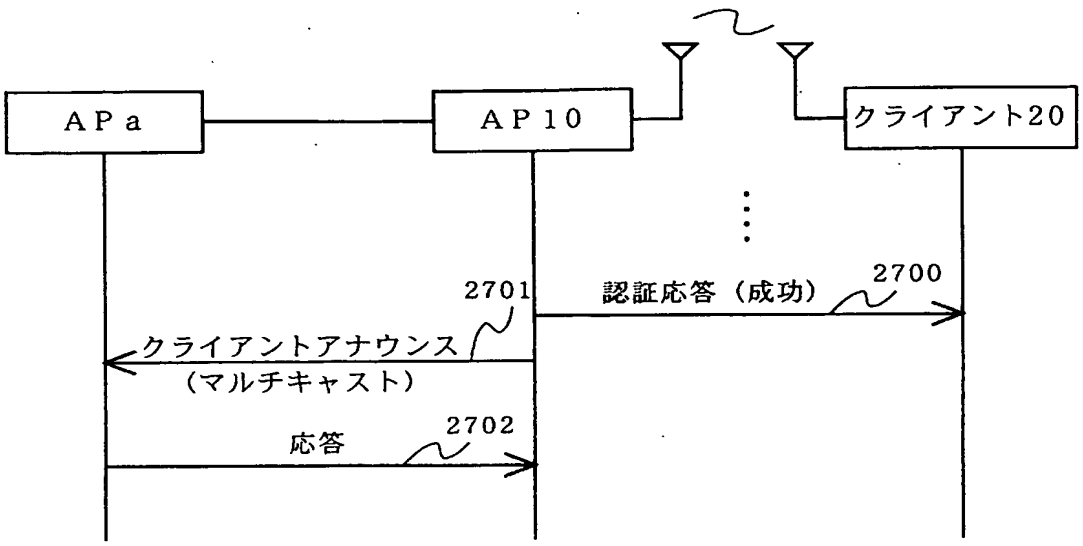
[図25]


ＡＰ１０
クライアント２０
暗号鍵選択
暗号鍵選択
プローブ要求
プローブ応答
認証要求
チャレンジ指示
チャレンジを暗号化した認証要求
ユーザの目視認証
認証応答（成功or失敗）
アソシエーション要求（成功の場合）
アソシエーション応答（成功の場合）

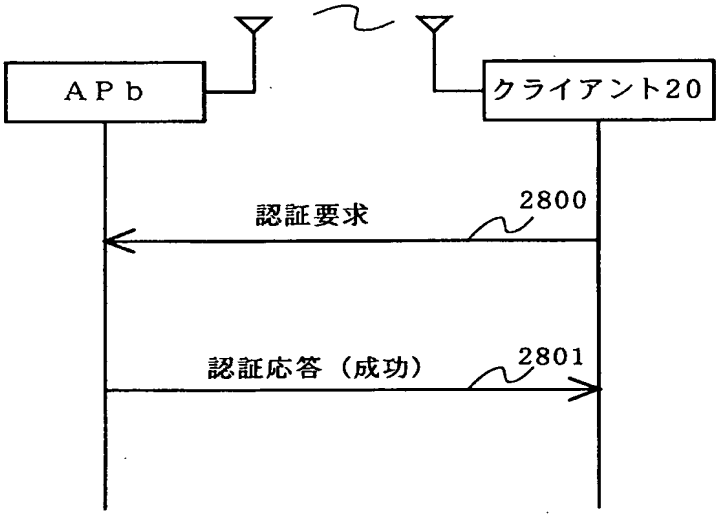
[図26]


ルータ
AP10
クライアント20
プローブ要求
プローブ応答
認証要求
認証要求
ユーザの
目視認証
認証応答
（成功or失敗）
認証応答（成功or失敗）
アソシエーション要求
（成功の場合）
アソシエーション応答
（成功の場合）

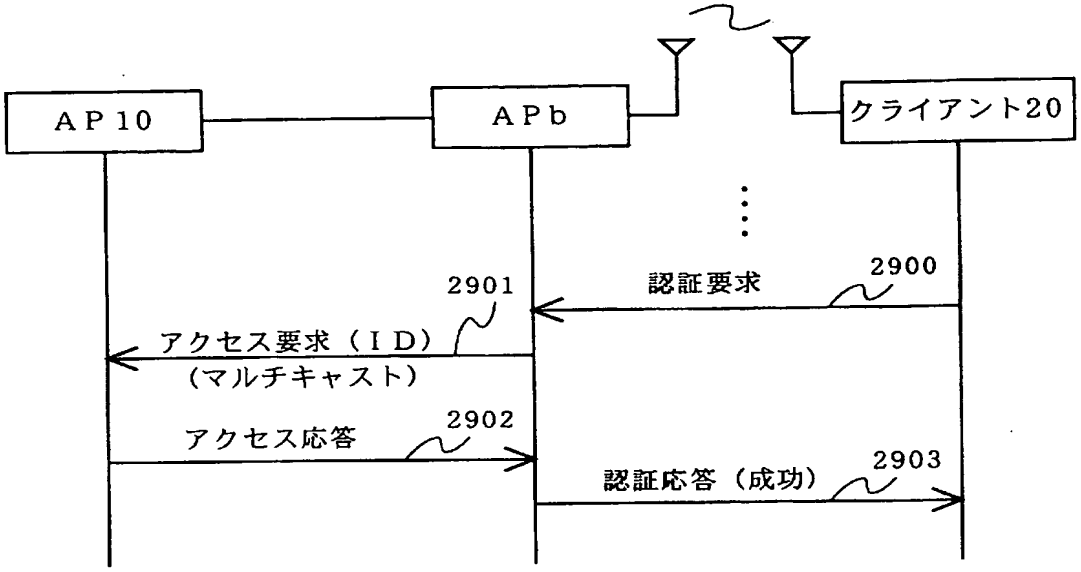
[図27]


APa
AP10
クライアント20
2701
認証応答（成功）
2700
クライアントアナウンス
（マルチキャスト）
応答
2702

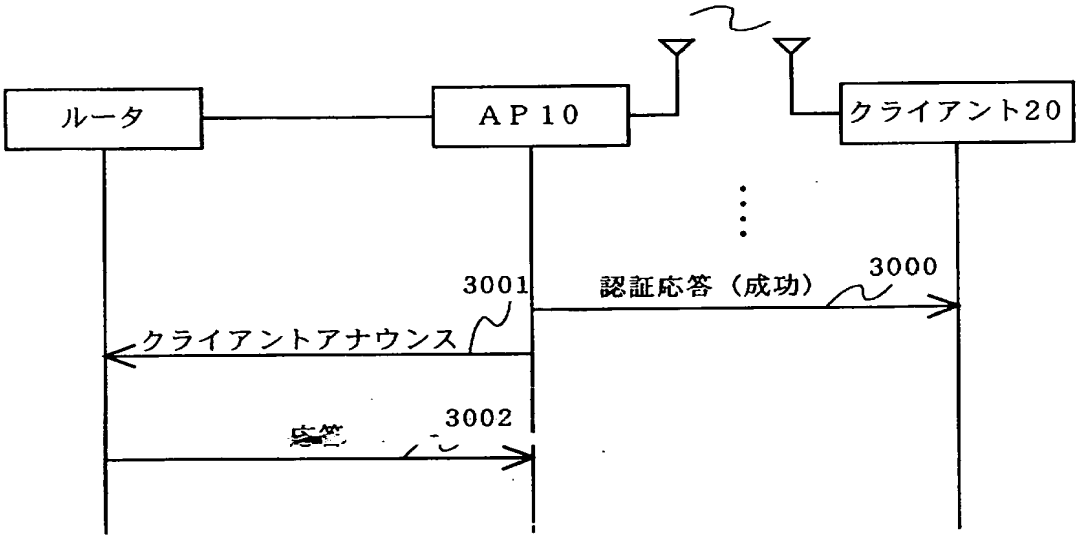
[図28]


APb
クライアント20
認証要求
2800
認証応答（成功）
2801

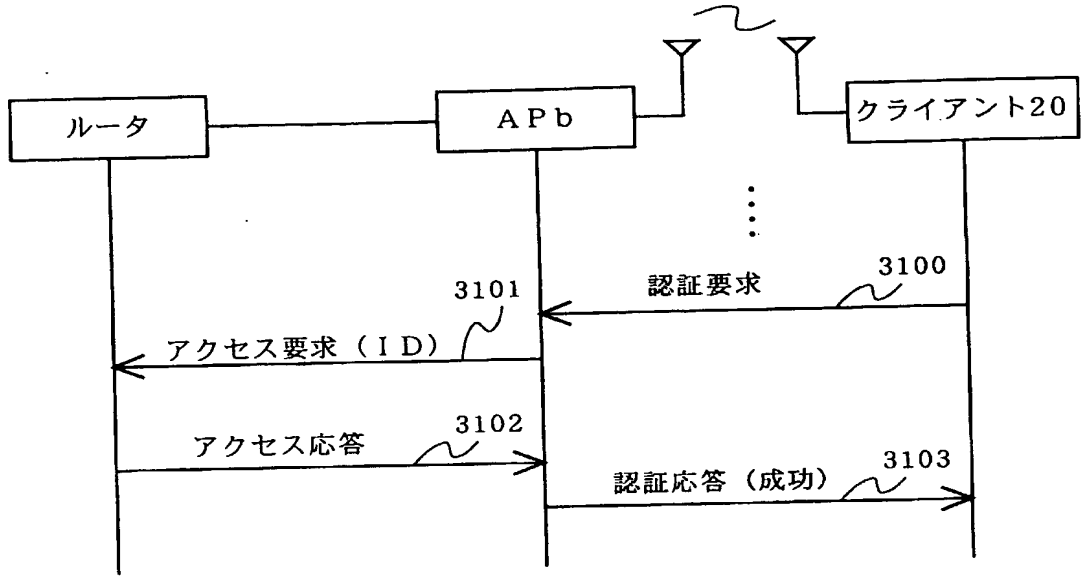
[図29]


AP10
APb
クライアント20
2900
認証要求
2901
アクセス要求（ＩＤ）
（マルチキャスト）
2902
アクセス応答
2903
認証応答（成功）

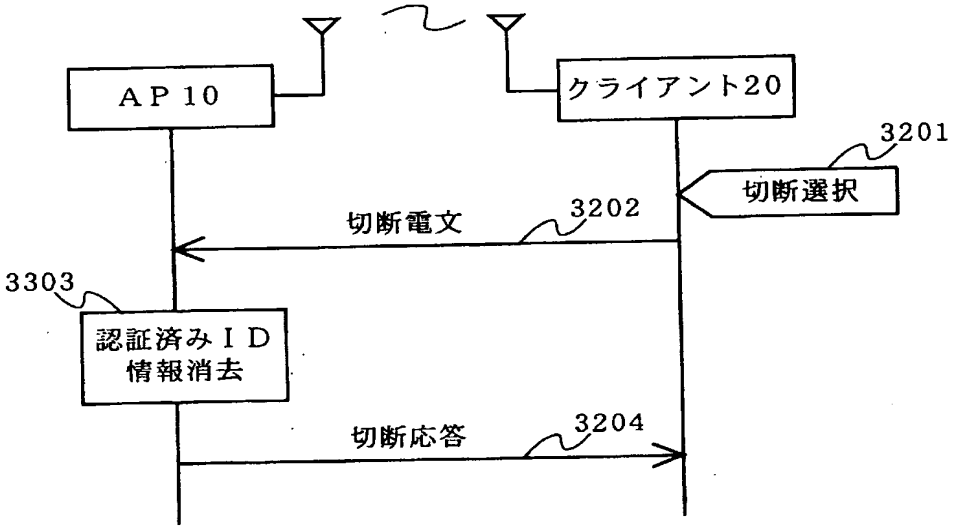
[図30]


ルータ
AP10
クライアント20
3000
認証応答（成功）
3001
クライアントアナウンス
3002
応答

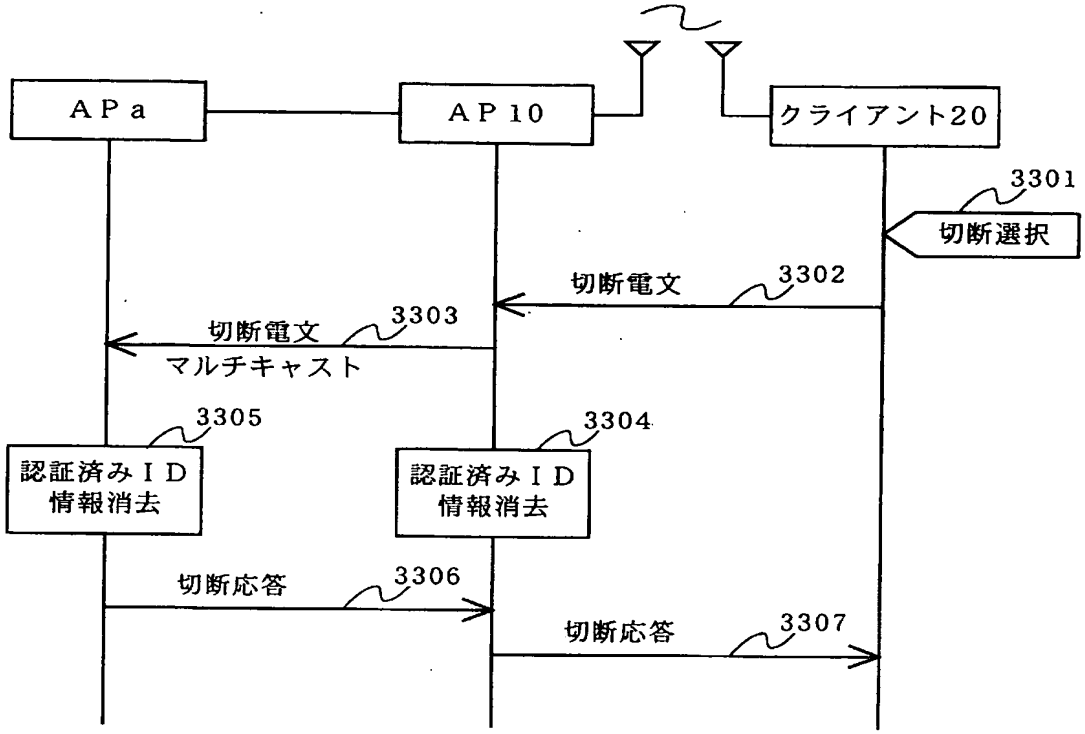
[図31]


ルータ
APb
クライアント20
3100
認証要求
3101
アクセス要求（ＩＤ）
3102
アクセス応答
3103
認証応答（成功）

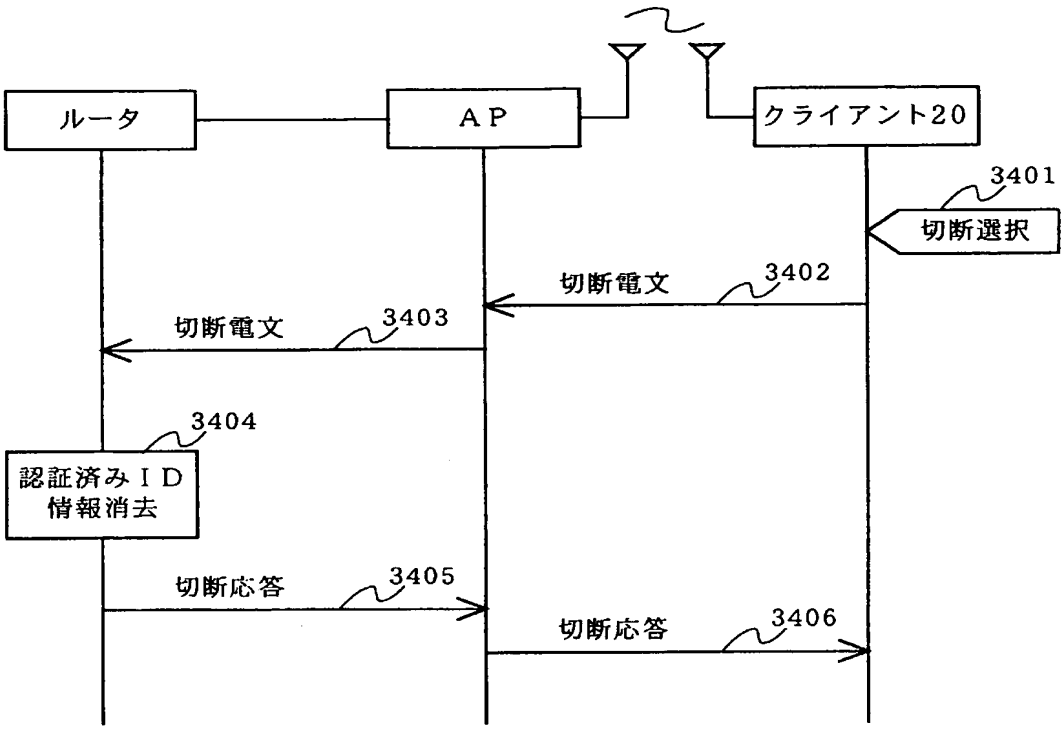
[図32]


AP10
クライアント20
3201
切断選択
切断電文
3202
3303
認証済みＩＤ
情報消去
切断応答
3204

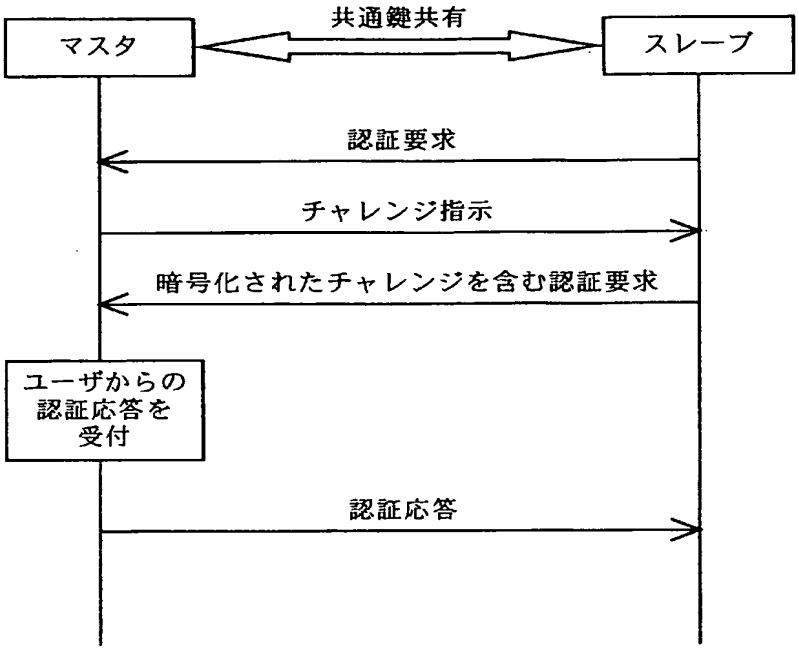
[図33]


ＡＰａ
ＡＰ１０
クライアント２０
3301
切断選択
切断電文
3302
切断電文
3303
マルチキャスト
3305
認証済みＩＤ
情報消去
3304
認証済みＩＤ
情報消去
切断応答
3306
切断応答
3307

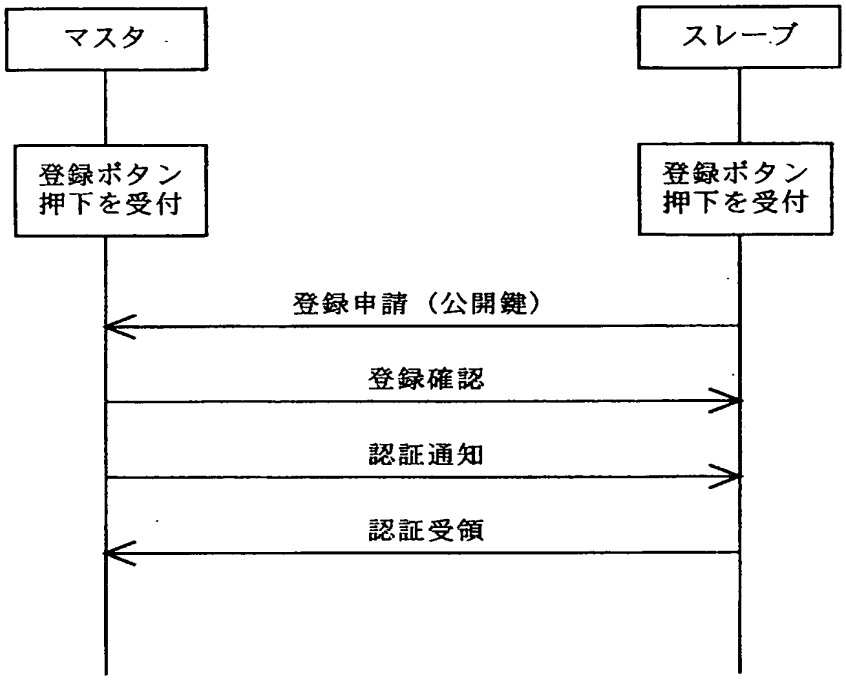
[図34]


ルータ
AP
クライアント20
3401
切断選択
切断電文
3402
切断電文
3403
3404
認証済みＩＤ
情報消去
切断応答
3405
切断応答
3406

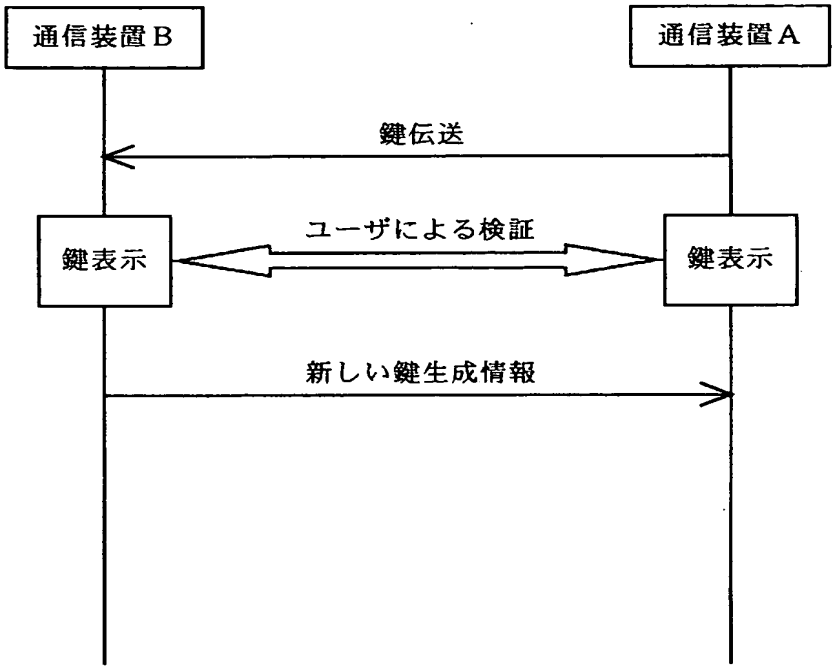
[図35]


共通鍵共有
マスタ
スレーブ
認証要求
チャレンジ指示
暗号化されたチャレンジを含む認証要求
ユーザからの
認証応答を
受付
認証応答

[図36]



[図37]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007096

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/32, H04L12/28, H04Q7/38, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/32, H04L12/28, H04Q7/38, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-313237 A (Minolta Co., Ltd.), 09 November, 1999 (09.11.99), Full text; Figs. 1 to 8 (Family: none)	1-14
Y	JP 2003-037592 A (Sharp Corp.), 07 February, 2003 (07.02.03), Par. Nos. [0009] to [0010], [0013] to [0016]; Figs. 1, 3 (Family: none)	1-14
Y	JP 11-030953 A (Hitachi, Ltd.), 02 February, 1999 (02.02.99), Par. No. [0009] (Family: none)	5,6

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 06 July, 2005 (06.07.05)	Date of mailing of the international search report 26 July, 2005 (26.07.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/007096

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-271318 A (Mitsubishi Materials Corp.), 20 September, 2002 (20.09.02), Par. Nos. [0022] to [0024]; Fig. 4 (Family: none)	7-10

国際調査報告

国際出願番号　PCT／JP2005／007096

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, H04L12／28, H04Q7／38, G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／32, H04L12／28, H04Q7／38, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　11－313237　A（ミノルタ株式会社） 1999．11．09　全文，図1－8 （ファミリーなし）	1－14
Y	JP　2003－037592　A（シャープ株式会社） 2003．02．07 第【0009】－【0010】段落， 第【0013】－【0016】段落，図1，3 （ファミリーなし）	1－14

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 06．07．2005	国際調査報告の発送日　26.07.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5S　4229 青木　重徳 電話番号　03－3581－1101　内線　3584

様式PCT／ISA／210（第2ページ）（2004年1月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　１１－０３０９５３　Ａ（株式会社日立製作所） １９９９．０２．０２　第【０００９】段落 （ファミリーなし）	５，６
Ｙ	ＪＰ　２００２－２７１３１８　Ａ（三菱マテリアル株式会社） ２００２．０９．２０ 第【００２２】－【００２４】段落，図４ （ファミリーなし）	７－１０